序　言

自从我的《有限群引论》第一次出版后的二十五年来，群论教学日益普及，教学内容也变得更加丰富．现在，群论是每一个数学系学生的必修课，这门课程的基本概念成为教育学院教师进修的内容之一，而且，在近代学校教学计划中，群论是通常设立的一门课程．由于人们对群论热烈和普遍的兴趣，那个教本显得过时是不足为奇的．它的这一缺点不易于用修订本来改正．

这本《群论引论》有了崭新的开端：引进了最新的术语和记号；不着重讨论有限群（象书名所指出的那样）；增添了一些新论题的简单内容，比如中心群列和幂零群．尽管有这些改变，我仍尽力保留了旧书的初等的特点．前几章应该能为有钻研精神的中学六年级学生所接受．全书打算包括对优等生开设的群论课程的大部份内容．象先前一样，当我相信另一条路径更富于启发性和更有教益时，我不总是挑选最短的途径去达到某一特殊的目标．在书末列举了一些内容更高深和更充实的教材，我希望，读者为了更深入地学习群论会去参考这些书．

这些年来，我收到过许多对于前一本书的建议和批评．所有这些意见都是有益的，而且只要可能，本书都采纳了．不过，我特别感谢J. A. 格林教授，他很细心地看了我的手稿，提出了非常宝贵的意见，这些意见反映了他在这领域中突出的专长和丰富的经验．

最后，我十分感谢出版者，感谢他们的好意和协作．

W. 莱德曼

目　　录

第一章 群的概念

§1. 引言. 算术的基本运算在于按照某些确定的规则结合两个数 a 与 b，以便得出一个唯一的数 c. 例如，假如合成规则是乘法，就有 $c=ab$. 当 a 与 b 给定时，数 c 总是能够得出的.

我们知道，两个或更多的数相乘服从某些形式法则，这些法则对所有的乘积都适用，而不论它们的数值怎样，比如

$$ab=ba \qquad \text{(交换律)} \tag{1.1}$$

$$(ab)c=a(bc) \text{(结合律)} \tag{1.2}$$

$$1a=a1=a. \tag{1.3}$$

最后一个等式引入了一个特殊的数，称为单位元素. 第二个法则更明确地说是这样的：假如我们令 $ab=s$ 及 $bc=t$，那么 $sc=at$ 就总是正确的.

在算术的公理方法中，习惯于一开始就规定公设或公理，例如(1.1)，(1.2)和(1.3)，以及另外某些关于加法和乘法的公设或公理，然后推演出这些公设的逻辑推论. 在开始时，不管这些记号 $a,b,\cdots$ 代表我们通常所理解的数，或者代表另外一些数学实体，或者实际上它们是否容许作任何具体的解释，都是没有关系的. 许多公理系统逻辑上都是可能的，但是它们不是同样的有趣或同样的有意义. 正是由于公理系统在纯粹数学或应用数学中应用的广度和深度的不同，使得我们选择某一个公理系统而不选择另一个.

§2. 群论公理. 群的抽象理论论述有限或无限的元素集

$$G: a,b,c,\cdots.$$

关于它规定了一个单一的合成规则，通常(虽然不总是)约定采用乘法的记号和术语来表示元素的合成. 因而我们假定对于 G 的任

意两个相等或不相等的元素 a,b,具有一个唯一的乘积 c,写作

$$ab=c.$$

按照更形式的说法,即元素的每一有序对 (a,b) 与一个唯一的元素 c 相联系. 有序对这个术语的意义是,当 $a\neq b$ 时,对 (a,b) 与对 (b,a) 是不同的. 两个元素的乘积仍然是群的一个元素,这是群的一个本质特征. 或者用更专门的术语来说,群关于乘法是封闭的. 群中所用的乘法类型必须服从在下面的定义中陈述的某些公理.

定义 1 对于一个集 G 规定了一个合成规则(乘法),假如下面的条件满足,那么这个集 G 形成一个群:

I. 封闭性 对 G 中每一有序对 a,b,都结合着 G 中唯一的一个元素 c,记作

$$ab=c,$$

c 称为 a 与 b 的积.

II. 结合律 假如 a,b,c 是 G 的任意三个元素,那么

$$(ab)c=a(bc).$$

因此两边都可以用 abc 表示.

III. 单位元素 集合 G 包含一个元素 1,称为**单位元素**(或**恒等元素**或**中性元素**),使得对于 G 的每一元素 a,有

$$a1=1a=a.$$

IV. 逆元素 对应 G 的每一元素 a,G 中存在一个元素 a^{-1},使得

$$aa^{-1}=a^{-1}a=1.$$

可以看出,除了一般不要求交换律对群适用之外,这些公设与熟知的数系,例如有理数系中乘法服从的那些规则很相似.

定义 2 假如一个群具有附加的性质,即对于它的任意两个元素 a,b,有

$$ab=ba,$$

那么这群称为**阿贝尔***(或**交换**)群.

在群中不要求交换律就必须区别 ab 与 ba. 我们分别称它们为用 b 后乘(或右乘)与前乘(或左乘)a. 当交换律在群中不是处处成立时,它们仍可以适用于某些特殊的元素对.

定义 3 元素 a,b 称为**交换**(或**可交换的**),假如

$$ab=ba.$$

例如,1 与每一元素交换;象 IV 中所要求的那样,a 总是与 a^{-1} 交换.

我们现在要从公理中引出某些结论,它们将进一步阐明群的结构.

(i) 结合律只对三个元素而假设,但是将会看到,n 个因子(按一定次序给出)的乘积具有唯一的意义,因而只要这些因子保留所给的次序,括号可以任意写进或省略. 因为,利用公理 II 作为归纳法的基础,我们可以假设少于 n 个因子的乘积已经有了定义,以及

$$a_1a_2\cdots a_r=(a_1a_2\cdots a_s)(a_{s+1}\cdots a_r),\text{此处 } 1<s<r<n.$$

需要证明

$$(a_1\cdots a_r)(a_{r+1}\cdots a_n)=(a_1\cdots a_s)(a_{s+1}\cdots a_n), \quad (1.4)$$

这意味任意两个不同的括号方式导致相同的结果. (1.4) 式的左边可以写成

$$[(a_1\cdots a_s)(a_{s+1}\cdots a_r)](a_{r+1}\cdots a_n)=[b_1b_2]b_3,$$

此处圆括号内的乘积分别用 b_1,b_2 与 b_3 表示. (1.4) 式右边第二个因子由于归纳假设被分开之后,(1.4)式右边可以表示为

$$(a_1\cdots a_s)[(a_{s+1}\cdots a_r)(a_{r+1}\cdots a_n)]=b_1[b_2b_3].$$

由公理 II 我们得到

$$[b_1b_2]b_3=b_1[b_2b_3],$$

这就证明了(1.4)式. 因此我们完全可以省略括号而把每边表为

* 为纪念 N. H. Abel(1802—29)而命名.

$$a_1a_2\cdots a_n.$$

特别，当所有因子都相同时，象在普通代数中那样，我们就写成

$$aa \qquad\qquad = a^2,$$

$$(aa)a = a(aa) = a^3,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

因而，当 n 与 m 是正整数时，我们有

$$a^m a^n = a^n a^m = a^{m+n} \tag{1.5}$$

及

$$(a^m)^n = a^{mn}. \tag{1.6}$$

我们有趣地看到，熟知的指数定律(1.5)和(1.6)最终是依靠乘法的结合律.

不过，当 a 与 b 不交换，通常会发现

$$(ab)^n \neq a^n b^n.$$

但是，当 a 与 b 交换时，

$$(ab)^n = abab\cdots ab = a^n b^n \tag{1.7}$$

及

$$a^m b^n = b^n a^m.$$

因为在这情况下我们可以任意地排列因子.

(ii) 公理 III 假定存在一个双边单位元素. 我们现在将证明只能有一个这样的元素. 因为假设$1'$是另一元素，具有与 1 相同的性质. 那么因为 $1'$作为右单位元素作用在 1上，$11'=1$，又因为 1 作为左单位元素作用在 $1'$上而有 $11'=1'$. 因此 $1=1'$.

(iii) 公理 IV 中所假设的(双边)逆元素是唯一的. 因为假设 $aa_1=1$，那么 $a^{-1}aa_1$ 可以用两种方法去计算，即

$$a^{-1}aa_1 = (a^{-1}a)a_1 = 1\,a_1 = a_1$$

及

$$a^{-1}aa_1 = a^{-1}(aa_1) = a^{-1}\,1 = a^{-1},$$

从而 $a_1 = a^{-1}$. 类似地，方程 $a_2a=1$ 意味 $a_2=a^{-1}$. 事实上，我们

已经证明 a 的任一左逆元素和 a 的任一右逆元素都等于 a^{-1}.

方程

$$ax=b, \quad ya=b$$

分别有解

$$x=a^{-1}b, \quad y=ba^{-1}.$$

一般情况中 $x\neq y$,我们必须区别用 a 左除与用 a 右除. 这些解是唯一的,因为假如

$$ax=ax_1=b,$$

那么,用 a^{-1} 左乘得出 $x=x_1$. 同样,如果

$$ya=y_1a=b,$$

我们推断出 $y=y_1$.

换句话说,我们有:在每一个群中,**消去律**既对于左消去又对于右消去成立.

显然

$$1=1^2=1^3=\cdots=1^n, \tag{1.8}$$

此处 n 是任一正整数. 因为 a 与 a^{-1}交换,我们从(1.8)和(1.7)得到

$$1^n=1=(aa^{-1})^n=a^n(a^{-1})^n.$$

由于逆元素的唯一性,$(a^{-1})^n$ 是 a^n 的逆元素,通常写为

$$(a^n)^{-1}=(a^{-1})^n=a^{-n}. \tag{1.9}$$

对任一元素 a 令

$$a^0=1. \tag{1.10}$$

读者不难确信,当 m 与 n 是任何正整数,负整数或零时,法则(1.5)与(1.6)仍然是有效的. 特别,我们看到同一元素的两个幂永远交换,甚至指数是负或零时也如此,因此

$$a^ka^l=a^la^k. \tag{1.11}$$

假如 a 与 b 是任意两个元素,我们有

$$(ab)(b^{-1}a^{-1})=abb^{-1}a^{-1}=1,$$

从而，由于逆元素的唯一性，

$$(ab)^{-1}=b^{-1}a^{-1}. \tag{1.12}$$

更一般地，有

$$(ab\cdots st)^{-1}=t^{-1}s^{-1}\cdots b^{-1}a^{-1}. \tag{1.13}$$

最后，我们说 1 是群的唯一的**幂等**元素，即方程

$$x^2=x \tag{1.14}$$

的唯一解是 $x=1$.

因为对(1.14)左乘以 x^{-1}，我们得到

$$x^{-1}x^2=x^{-1}x,$$

因而

$$x=1\ .$$

假如 G 包含有限个元素，那么元素的个数称为 G 的**阶**；否则 G 称为无限阶的群. G 的阶，不论有限或无限，都用

$$|G|$$

来表示.

虽然对于群的元素的合成常采用乘法这一术语，但是有时为了方便，也采用另外的记号. 比如用

$$a\circ b$$

表示 a 与 b 的合成.

当群是阿贝尔群时(本书中只在这种情况下)经常喜欢用加法记号. 因此对于 a 与 b 的合成我们写成

$$a+b(=b+a),$$

结合律写成

$$(a+b)+c=a+(b+c).$$

单位元素(中性元素)用 0 表示，因此

$$a+0=0+a=a,$$

逆元素写成$(-a)$. 类似 a 的幂，现在就是

$$a+a+\cdots+a=na,$$

此处左边包含 n 个相同的项. 要注意右边的整数 n 通常不是群的元素,事实上,na 只是等式左边的缩写. "指数律"现在采取如下形式:

$$(n+m)a=na+ma,$$
$$n(ma)=(nm)a.$$

我们引入记号

$$-(na)=(-n)a.$$

因为是阿贝尔群,所以我们有更进一步的关系

$$n(a+b)=na+nb.$$

§ 3. 群的一些例子. 群在大多数数学分支中是屡见不鲜的. 这里我们搜集了几个群的例子,读者可能在别的地方遇见过它们.

(i) *所有正有理数集对于乘法形成一个群.* 的确,两个正有理数的积还是一个正有理数,单位元素是有理数 1,正有理数的逆元素也是正有理数. 结合律作为算术中的一个法则已为人们所知道. 这是一个无限阿贝尔群. 明显地,负有理数集不能形成群;正整数集也不能形成群,因为除 1 之外的每一个元素都没有逆元素.

(ii) *所有整数集对于加法形成一个阿贝尔群.* 这群通常以 Z 表示.

(iii) *围绕一固定点的旋转:* 假如一个三维的刚体相对于一固定点 O 自由转动,则刚体的每一位移相当于围绕经过 O 的一条线 l 转动一角度 α. 这样的位移将用(l,α)表示,或者更简单地用一个单一的字母 $a=(l,\alpha)$来表示. 假如 b 是另一个相对 O 的位移,乘积 ab 规定为这样一个位移,它是 b 跟随 a 之后的结果(按照这个次序——有些作者喜欢用相反的规定,依照那种规定,积必须从右向左念). 在这合成规则下,关于 O的所有位移的集形成一个非阿贝尔群. 单位元素的作用可以表示为$(l,0)$,此处 l 是任意的,(l,α)的逆元素是$(l,-\alpha)$. 根据转动是一种特殊的线性

变换这一事实可得出结合律.

我们通常只对使物体与自身重合的那些位移感兴趣,位移的这样的子集也形成一个群,它称为物体的**对称群**.

下面的实例说明交换律不总是能满足的. 设 1 2 3 4 表示一正方形薄板,最初放在(x,y)-平面内,如图 1 所示,z 轴与薄板平面成直角. 我们假设 $Oxyz$ 是一个右手参考系,它固定在空间中.

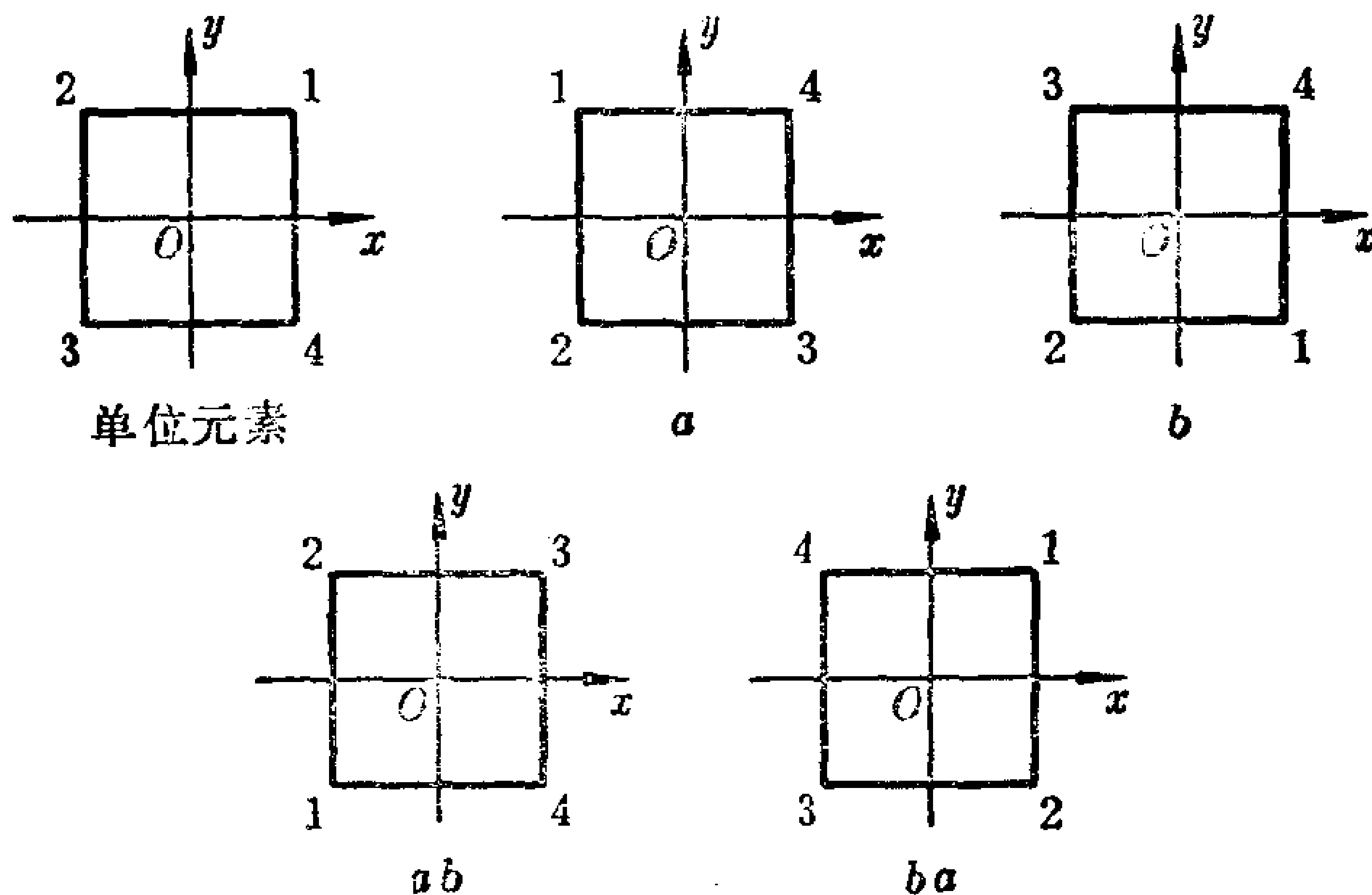


图 1

假如用上面的记号,则有

$$a=\left(Oz,\ \frac{1}{2}\pi\right),\qquad b=(Ox;\pi).$$

从最后的两个图可以看出 ab 与 ba 造成薄板的不同位置.

(iv) 矩阵群：读者要熟悉基本的矩阵代数,特别要熟悉矩阵乘法. 群的一些最重要的例子是由矩阵的某些集提供的.

(a) 设 F 是一个域,例如实数域,考虑所有非奇异 $n\times n$ 矩阵,它的元素可从 F 中任意选择. 这个集在矩阵的乘法下形成一个群. 它用 $GL(n,F)$来表示,称为 F 上 n 次的**一般线性群**.

(b) 所有 F 上 n 阶正交矩阵在矩阵乘法下形成一个群.

(c) 元素是整数的非奇异 $n\times n$ 矩阵集在乘法下是封闭的，但是这样的矩阵的逆元素一般不属于这个集，因为这个逆元素的形成需要用行列式去除. 可是，行列式是 ± 1 的整数矩阵集的确形成一个群，它称为 n 次幺模群*.

(v) 剩余类：设 m 是大于 1 的固定整数，在本文中 m 称为模. 假如 $x-y$ 可以被 m 整除，那么两个整数 x 与 y 就称为关于模 m 同余，或者称为模 m 同余，这用符号写成

$$x\equiv y(\operatorname{mod} m). \tag{1.15}$$

这相当于说：存在一个整数 k 使得

$$x=y+km. \tag{1.16}$$

例如，$3\equiv 18(\operatorname{mod} 5)$，$-2\equiv 14(\operatorname{mod} 8)$，$12\equiv 0(\operatorname{mod} 3)$.

任何一个整数都恰与集

$$Z_m,0,1,2,\cdots(m-2),(m-1) \tag{1.17}$$

中的某一个整数模 m 同余. 因而 Z_m 被称为模 m 的完全剩余集. 事实上这些数是模 m 的最小非负剩余.

容易检验下面关于同余的法则：

假如 $x_1\equiv y_1(\operatorname{mod} m)$ 及 $x_2\equiv y_2(\operatorname{mod} m)$，那么

$$x_1+x_2\equiv y_1+y_2\ (\operatorname{mod} m) \tag{1.18}$$

及

$$x_1x_2\equiv y_1y_2\ (\operatorname{mod} m). \tag{1.19}$$

由于(1.18)，我们能用下面的规定赋予 (1.17) 一个加法群结构，这个规定是：$a+b$ 是(1.17)中与 $a+b$ 模 m 同余的元素，换句话说，元素的合成是普通的加法，假如和大于 m，就将元素的和约化到模 m 的最小非负剩余. 单位元素是零，a 的逆元素是$(m-$

---

* 有些作者只对行列式等于 1 的矩阵用这名词.

a). 因而 Z_m 是一个群;它称为模 m 剩余类的加法群. 例如,当 $m=5$, $1+2=3$, $3+4=2$, $2+3=0$ 等等.

也许会问,是否可以用相似的方法利用(1.19)在剩余集中引入一个乘法群结构. 但是不久就会明白,即使我们略去零剩余——它明显地不能是阶大于1的乘法群的元素——我们也将要陷入困境. 象我们在§2中所看到的那样,消去律要求假如 $cx=cy$ 则 $x=y$. 但是, 例如, 我们有 $22\equiv4(\bmod 6)$,而 $11\not\equiv2(\bmod 6)$,所以消去律对于模 m 的乘法一般并不成立. 尽管如此,我们将看到,同余式中的消去律在某些情况下是容许的. 为了分析这种情况,我们需要从初等数论中借用一些结果和记号:a 与 b 的最大公约数用(a,b)表示; 特别, 当$(a,b)=1$ 时, 我们说 a 与 b **互素**. 如果 a 能整除 b,我们写成 $a|b$. 下面的事实只引用不证明.

(i) 假如 $m|kc$ 及$(m,k)=1$,那么 $m|c$.

(ii) 假如$(m,a)=1$ 及$(m,b)=1$,那么$(m,ab)=1$.

(iii) 假如$(m,a)=1$.那么存在整数 u 与 v 使得 $au+mv=1$.

现在我们可以说:假如$(k,m)=1$, 那么由于同余式

$$kx\equiv ky(\bmod m) \tag{1.20}$$

可得 $x\equiv y(\bmod m)$. 因为 (1.20)相当于 $m|k(x-y)$, 从而由(i), $m|(x-y)$. 即 $x\equiv y(\bmod m)$. 因此假如某一因子与模互素. 它就可以消去.

在集

$$1,\ 2\cdots,\ m$$

中那些与 m 互素的整数个数用$\phi(m)$(**欧拉函数**)表示.例如,$\phi(9)=6$, 因为有6个整数 n 使得 $1\leqslant n\leqslant 9$ 及 $(n,9)=1$. 当 p 是素数时, 在集 $1, 2,\cdots, p$ 的所有整数中, 除最后一个整数外,

都与 p 互素，因此

$$\phi(p)=p-1. \tag{1.21}$$

还有，当 $m=p^r$ 时，此处 r 是正整数，集 $1,2,\cdots,p^r$ 中只有 p 的倍数不与 p 互素. 因为共有 p^{r-1} 个 p 的倍数，所以

$$\phi(p^r)=p^r-p^{r-1}. \tag{1.22}$$

通常约定

$$\phi(1)=1. \tag{1.23}$$

一般地，令

$$R_m: a_1, a_2, \cdots, a_{\phi(m)} \tag{1.24}$$

为与 m 互素的最小的正剩余集，因而 $(a_i,m)=1$ 及 $0<a_i\leqslant m$. 其中某一剩余，比如说 a_1，等于 1. 由(ii)，(1.24) 中任意两个元素的积还与 m 互素；当这积大于 m 时，它就不包括在(1.24)内而与(1.24)中的某一个元素同余. 事实上任意一个与 m 互素的整数都是这样，因此我们可以写成

$$a_i.a_k\equiv a_l(\bmod m), \tag{1.25}$$

且在 R_m 中用乘法这样来定义一个合成法则：如果必要，就将乘积约化到模 m 的最小正剩余，例如

$$4\times 5\equiv 2(\bmod 9), \quad 4\times 7\equiv 1(\bmod 9).$$

假如已经明白我们只在模 m 算术中运算，使得等式只适用于模 m，那么简单地将 R_m 中的乘法表达如下是合适的，

$$a_ia_k=a_l. \tag{1.26}$$

从同余式的性质易于推导出 R_m 中交换律和结合律是满足的，也很清楚 $1\,(=a_1)$ 是单位元素. 剩下需要证明每一元素 $a\in R_m$ 具有一逆元素. 既然 $(a,m)=1$，我们能够应用(iii)推出下面形式的等式的存在，

$$au+mv=1. \tag{1.27}$$

这相当于 $au \equiv 1 (\bmod m)$. 因此 u 是 R_m 中 a 的逆元素. 因而在所指定的合成规则下, R_m 形成一个 $\phi(m)$阶的阿贝尔群.

§ 4. 乘法表. 在群的抽象理论中是不提元素性质的. 假如所有可能的乘积都知道或者能够用指定的法则决定, 那么这个群就完全给定了. 在 g 阶的有限群中共有 g^2 个这样的乘积, 它们可以方便地列入一个 $g \times g$ 的乘法表中, 象凯莱*(A.Cayley)首先提出的那样. 下面的表分别显示 2, 3 和 4 阶的群.

(i)

	1	a
1	1	a
a	a	1

(ii)

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	~~b~~ a

(iii)

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

(iv)

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

在上面每一种情况中,乘积 $x\ y$ 都安置在用 x 标示的行和用 y 标示的列的交点上. 例如,在(iii)中, 我们有 $ac=b$, 而在 (iv) 中,$ac=1$. 读者会看到这些群都是阿贝尔群,这一点由下面的事实显示出来, 即这些表对于从西北到东南的对角线都是对称的.

下面的群提供了一个更有启发性的例子.

$$G:1,a,b,c,d,e \tag{1.28}$$

是 6 阶群, 具有下面的乘法表

* Phil.Mag.,vol. Vii(4), 1854.

(v)

	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	b	1	e	c	d
b	b	1	a	d	e	c
c	c	d	e	1	a	b
d	d	e	c	b	1	a
e	e	c	d	a	b	1

(1.29)

这个表使得群的某些性质成为明显．封闭性是明显的，因为每一项都是(1.28)中的元素；单位元素的作用相当于这件事实：即方表中第一行和第一列由(1.28)中的元素按原来次序排列而成；对于每一元素存在一个逆元素以及逆元素的值都是明显的，因为在每一行每一列中只有一项等于1．只是验证结合律有些困难．对所有 x,y 和 z 验算 $x(yz)=(xy)z$ 是一件吃力的工作，即使对于一个小的群也是如此．在上面的表中，结合律的确成立，例如

$$(ac)d=ed=b, \qquad a(cd)=a^2=b,$$

但是它的普遍有效最好用间接的论证来证实，这一点一会儿就说明．

一个正方形的表，它的每一行每一列都由按某种次序排列的同样的元素组成，有时被称为**拉丁方**．因而有限群的乘法表总是一个拉丁方，但是反过来就不一定对，因为结合律可能不满足．例如下面 5 × 5 的拉丁方

	1	a	b	c	d
1	1	a	b	c	d
a	a	1	d	b	c
b	b	c	1	d	a
c	c	d	a	1	b
d	d	b	c	a	1

不能解释为某个群的乘法表，因为$(ab)c=dc=a$，而$a(bc)=ad=c$，与结合律矛盾.

容易验证下面六个矩阵的集

$$\Gamma:\begin{cases} I=\begin{bmatrix}1&0\\0&1\end{bmatrix}, A=\begin{bmatrix}-1&-1\\1&0\end{bmatrix}, B=\begin{bmatrix}0&1\\-1&-1\end{bmatrix}, \\ C=\begin{bmatrix}0&1\\1&0\end{bmatrix}, D=\begin{bmatrix}1&0\\-1&-1\end{bmatrix}, E=\begin{bmatrix}-1&-1\\0&1\end{bmatrix}, \end{cases} \tag{1.30}$$

对于矩阵乘法是封闭的. 例如

$B=A^2$，$A^3=C^2=D^2=E^2=I$，$AD=C$，$AC=E$，等等. 此外，我们会发现整个6×6乘法表与(1.29)全同，只要用I代替1，用大写字母代替小写字母. 因此，假如按照(1.29)，$xy=z$，Γ中对应的矩阵就满足关系式$XY=Z$. 相反地，Γ中任意一个乘法关系将与G中对应的关系配对. 但是我们已经知道矩阵乘法是结合的，即对于Γ中任意三个元素，有$(XY)Z=X(YZ)$. 因而我们证明了$(xy)z=x(yz)$在G中也成立. 因此我们也就在G中证实了结合律. 上面这种情况可这样来描述：Γ提供了一个G的**忠实表示**. 这是一个例子，说明抽象群论受到了更具体的数学知识的帮助.

我们可以说G和Γ具有相同的结构. 这是一个重要概念的具体说明. 下面我们就来详细地阐明这个概念. 设

$$G:1,a,b,c,\cdots \tag{1.31}$$

及

$$G':1',a',b',c',\cdots \tag{1.32}$$

是两个(有限或无限)群，此处G与G'的单位元素分别用1和$1'$表示. 假设G的元素与G'的元素之间存在一个一一对应

$$\theta:G\longleftrightarrow G', \tag{1.33}$$

就是说对于G中每一元素x，我们在G'中指定一个唯一的象x'

$=x\theta$，以及 G' 中每一元素 y' 是 G 中唯一的元素 y 的象，因此 $y'=y\theta$. 换句话说，G 的元素和 G'的元素以这样方式配对，使得 G 与G' 的每一元素恰在一对中出现. 此外，假设这个对应具有性质：$xy=z$ 当且仅当 $x'y'=z'$；或者，更正式地写成

$$(xy)\theta=(x\theta)(y\theta). \tag{1.34}$$

则我们就说 G 与 G' 是**同构的**(*isomorphic*，即"形状相同"的希腊语)，我们写成

$$G\cong G'. \tag{1.35}$$

G 的元素之间的任一关系对应于 G'的元素之间的一个关系，相反地，G' 的元素之间的任一关系对应于 G 的元素之间的一个关系. 简单地在元素符号上添上和去掉逗号，就可以从一个群变到另一个群. 这两个群只在记号上有区别，从抽象的观点来看，它们必须被看成是等同的，因为它们具有相同的乘法表. 用更专门的术语来说，在所有的群所形成的集中，同构概念构成一种等价关系. 因为通常那些条件明显地被满足：(i)$G\cong G$（自反性），(ii) 假如 $G\cong G'$，那么 $G'\cong G$(对称性)，(iii)假如 $G\cong G'$ 及 $G'\cong G''$，那么 $G\cong G''$(可递性). 下面我们再举几个例子以助于说明这个概念.

例 1 下面几个 4 阶群是同构的，每一个群的合成规则在括号内说明：

(1) 数$1,i,-1,-i$, （通常的乘法）

(2) 矩阵

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}0&1\\-1&0\end{bmatrix},\begin{bmatrix}-1&0\\0&-1\end{bmatrix},\begin{bmatrix}0&-1\\1&0\end{bmatrix},$$（矩阵乘法）

(3) 剩余 1，2，4，3(mod 5)， （模 5 的乘法）

假如在每一种情况中元素重新命名为 1，a，b，c，那么乘法表成为前面的表(iv).

例 2 下面的 4 阶群是同构的.

(4) 矩阵

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}1&0\\0&-1\end{bmatrix},\begin{bmatrix}-1&0\\0&1\end{bmatrix},\begin{bmatrix}-1&0\\0&-1\end{bmatrix},$$（矩阵乘法）

(5) 剩余 1,3,5,7 (mod 8)， （模 8 的乘法）

假如在每种情况中元素用 $1, a, b, c$ 标示，乘法表与前面的表(iii)相同.

显然，如果两个有限群是同构的，那么它们必须包含相同个数的元素．但是反过来就不一定对．例如，表(iii) 与表 (iv) 给出的群不是同构的，因为在(iii)中每一元素满足方程 $x^2=1$，在表(iv) 中就不是这样，所以同阶的群可以有不同的结构.

§ 5. 循环群. 考虑不同符号的集

$$C:1(=x^0),\ x,\ x^{-1},\ x^2,\ x^{-2},\ \cdots,\ x^n,\ x^{-n},\ \cdots, \tag{1.36}$$

对于这个集用下面的规则规定乘法

$$x^r x^s = x^{r+s} (r, s = 0, \pm 1, \pm 2, \cdots). \tag{1.37}$$

在这合成规则下，C 成为一个阿贝尔群，它称为由 x 生成的**无限循环群**．这个群与整数加法群同构，即与下面的集同构，

$$Z: 0, \pm 1, \pm 2, \cdots.$$

在 Z 中，r 与 s 的合成定义为 $r+s$．建立同构的对应 θ 由

$$x^r\theta = r$$

给出．可是，因为群 Z 是按加法合成写出的，所以此处(1.34)必须用下式代替

$$(x^r x^s)\theta = x^r\theta + x^s\theta.$$

因此，所有无限循环群都是同构的.

假设符号 x 满足方程式

$$x^m = 1, \tag{1.38}$$

此处 m 是比 1 大的整数，则将出现一个更有趣的情况．在这情况中，不同符号的集

$$C_m: 1, x, x^2, \cdots, x^{m-1} \tag{1.39}$$

形成一个 m 阶阿贝尔群，它遵循下面的合成规则

$$x^r x^s = x^{r+s} (r, s = 0, 1, \cdots, m-1),$$

此处 $r+s$ 必须约化到它的模 m 的最小非负剩余. 这个群称为由 x 生成的 m 阶**循环群**. 它与模 m 剩余类的加法群

$$Z_m: 0, 1, 2, \cdots m-1$$

同构,Z_m 曾经在 §3(v) 中描述过. 因而, 所有 m 阶循环群都是同构的.假如我们将(1.39)中的 x 用复数

$$\varepsilon = \exp(2\pi i/m)$$

代替,就可以得到这个群的另一种表示. 任意一个复数乘以 ε, 对应一个在复数平面上转动 $2\pi/m$ 的旋转. 如果这个运算重复 m 次,每一点将完成一个完全的循环,这就说明了循环群这名词的由来.

现在假设 x 是任意一个群的元素,那么可能出现两种情况:或者列举在(1.36)中的 x 的所有次幂彼此都不相同, 或者存在两个整数 k 与 l 使得 $k>l$,且

$$x^k = x^l,$$

因此

$$x^{k-l} = 1.$$

于是,在这种情况下, x 的某一正次幂等于单位元素, 因而一定存在一个 x 的最小正指数次幂等于单位元素. 这一点引导到下面的定义.

定义 4 设 x 为某一群的元素,假如所有 x 的幂彼此都不同,就说 x 是**无限阶**的. 假如 x 的各次幂不是都不相同, 那么存在一个最小的正整数 h,称为 x 的**阶**(**周期**),使得

$$x^h = 1.$$

当然,在有限群中,所有的元素都是有限阶的. 假如 x 是 h 阶元素,那么 $x^h=1$ 但是当 $0<k<h$ 时,$x^k \neq 1$. 还有,假如 $m=hg$,则我们有

$$x^m = (x^h)^g = 1.$$

这句话反过来说也是正确的.

命题 1 假如 x 是 h 阶的,那么 $x^m=1$, 当且仅当 m 是 h 的倍数.

证明 用 h 除 m,设 q 为商, r 为余数,因此

$$m=hq+r,$$

此处 $0\leqslant r<h$. 因而

$$1=x^m=(x^h)^q x^r=1\ x^r=x^r.$$

这一点与 h 的最小性相矛盾,除非 $r=0$. 因此

$$m=hq.$$

易于验证下面关于群的一个元素的阶的事实:

(i) 单位元素是唯一的一阶元素.

(ii) 元素 x 与 x^{-1} 有相同的阶.

(iii) 假如 $y=t^{-1}xt$,此处 t 是任意元素, 那么 x 与 y 是同阶的.

命题 2 设 x 是 h 阶元素. 假如 s 是某一正整数,那么 x^s 是 $h/(h,s)$阶元素,此处(h,s)表示 h,s 的最大公约数.

证明 设 $d=(h,s)$. 我们于是有

$$h=dh',\quad s=ds',$$

此处 $(h',\ s')=1$. 我们必须证明 x^s 是 h' 阶的. 现在 $(x^s)^{h'}=x^{s'dh'}=(x^{h'd})^{s'}=(x^h)^{s'}=1$,因为 x 是 h 阶的. 尚须证明, 假如 t 是任一正整数使得

$$(x^s)^t=1, \tag{1.40}$$

那么$t\geqslant h'$. 假设(1.40)正确,那么根据命题 1,$h|st$,即$h'd|s'dt$, 因此 $h'|s't$. 但是 h' 与 s' 互素. 因此 $h'|t$,从而 $h'\leqslant t$.

§ 6. 集的映射. 设$\Sigma:\xi,\eta,\zeta,\cdots$是对象的一个有限或无限集. Σ 到自身内的映射

$$f:\Sigma\to\Sigma$$

是一个法则,根据这法则,对于每一个$\xi\in\Sigma$,有一个唯一指定的对

象 $\eta\in\Sigma$，称为ξ在 f 下的象，我们宁愿写成$\eta=\xi f$，而不用记号 $\eta=f(\xi)$，因为后者更习惯于用在分析和拓扑中. 两个映射 f 与 g 是相等的，当且仅当对于所有的 $\xi\in\Sigma$，$\xi f=\xi g$. f 与 g 的合成是映射 $f\circ g$，规定为

$$\xi(f\circ g)=(\xi f)g,$$

它的意思是 $f\circ g$ 是 g 随 f 后而得到的映射，所以如果 $\xi f=\eta$，那么$\xi(f\circ g)=\eta g$.

设 f,g 与 h 是三个Σ 到自身内的映射，我们要证明这些映射的合成永远服从结合律. 设 ξ 是 Σ 的任一对象，令

$$\xi f=\eta,\quad \eta g=\zeta,\quad \zeta h=\tau.$$

那么

$$\begin{aligned}&\xi[f\circ(g\circ h)]=(\xi f)(g\circ h)=\eta(g\circ h)\\&=(\eta g)h=\zeta h=\tau\end{aligned}$$

及

$$\xi[(f\circ g)\circ h]=[\xi(f\circ g)]h=[(\xi f)g]h=(\eta g)h=\zeta h=\tau.$$

由于 ξ 是 Σ 的任意一个对象，所以可得

$$f\circ(g\circ h)=(f\circ g)\circ h. \tag{1.41}$$

例 1 设 Σ：$\xi,\eta,\zeta,\cdots$是一个 n 维向量空间. 我们可以把 Σ 的对象考虑为行向量. 假如 A 是 $n\times n$ 矩阵，那么 $f:\xi\to\xi A$ 是 Σ 到自身内的映射. 假如 $g:\xi\to\xi B$ 是另一个这样的映射，则合成映射就是 $f\circ g:\xi\to\xi AB$. 因此，上面的讨论证实了矩阵乘法是结合的.

为了证明映射的集

$$G: f,g,h,\cdots$$

形成一个群，我们只需要验证群的定义中的公理 (I)，(III) 与 (IV). 我们注意到，f 具有一个逆元素当且仅当 f 是一一的而且将 Σ 映射到自身上，这意味着每一个 $\eta\in\Sigma$，恰好是一个Σ中的对象 ξ 的象. 因此关系 $\xi f=\eta$ 可以对 ξ 唯一地解出，而写为 $\xi=$

ηf^{-1},因而定义了逆映射 f^{-1}.

例 2 使一给定的固体与自身重合的映射的集合明显地满足(I),(III)与(IV),因此形成一个群.

例 3 设 z 分布在扩充了的 z 平面上，即分布在所有的复数和无穷远点上. 六个映射

$$\left.\begin{aligned} &f_1: z\to z(\text{恒等映射}), f_2: z\to\frac{1}{1-z}, f_3: z\to\frac{z-1}{z},\\ &f_4: z\to\frac{1}{z}, f_5: z\to 1-z, f_6: z\to\frac{z}{z-1}\end{aligned}\right\} \quad (1.42)$$

将扩充了的 z 平面变换到自身内，因此这些映射在合成下构成一个结合的系统. 值得注意的是,这个系统是封闭的. 例如

$$z(f_2\circ f_3)=(zf_2)f_3=\frac{1}{1-z}f_3=\frac{(1-z)^{-1}-1}{(1-z)^{-1}}=z=zf_1,$$

所以 $f_2\circ f_3=f_1$,因而 $f_3=f_2^{-1}$.

$$z(f_4\circ f_3)=(zf_4)f_3=\frac{1}{z}f_3=\frac{z^{-1}-1}{z^{-1}}=1-z=zf_5$$

所以 $f_4\circ f_3=f_5$ 等等. 完整的乘法表如下：

(vi)

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_5	f_6	f_4
f_3	f_3	f_1	f_2	f_6	f_4	f_5
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_4	f_6	f_2	f_1	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

假如我们用 $1,a,b,c,e,d$* 代替 f_1,f_2,f_3,f_4,f_5,f_6，可以看出表(vi)与表(v)相同. 因此我们发现了这个抽象群的另一个忠实表

* 注意不是 $1,a,b,c,d,e$——译者

示.

§7. 置换. 研究作用在有限集 Σ 上的映射是特别重要的. 为简单起见,Σ 的对象经常用整数 $1,2,\cdots,n$ 表示. Σ 到自身上的映射称为 n **次置换**. 它用下面的符号明显地表示出来:

$$\pi=\begin{pmatrix}1 & 2\cdots & j & \cdots n \\ a_1 & a_2\cdots & a_j & \cdots a_n\end{pmatrix}, \tag{1.43}$$

此处 $a_j=j\pi$ 是 j 在 π 下的象. 因此 (1.43) 中的第二行是整数 $1,2,\cdots,n$ 的一个重新排列. 根据初等代数我们知道,共有 $n!$ 个这样的排列. 因此共有 $n!$个 n 次置换. 全部的置换集将以 S_n 表之.

我们注意到(1.43)所给出的置换可以用各种不同的等价方式表示出来. 事实上我们可以随意地安排(1.43)中的各列. 例如,下面的符号

$$\begin{pmatrix}1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4\end{pmatrix}=\begin{pmatrix}2 & 1 & 4 & 3 \\ 3 & 2 & 4 & 1\end{pmatrix}=\begin{pmatrix}4 & 2 & 1 & 3 \\ 4 & 3 & 2 & 1\end{pmatrix}=\cdots$$

全都表示同一个置换.这些符号中的第一个,顶上一行的对象按自然次序排列,称为**标准形式**. 明显地, 任一置换容许 $n!$个等价的形式, 因为顶上一行可以任意选择而第二行按规定相应地排列.

设

$$\rho=\begin{pmatrix}1 & 2 & \cdots n \\ b_1 & b_2 & \cdots b_n\end{pmatrix}=\begin{pmatrix}a_1 & a_2 & \cdots a_n \\ c_1 & c_2 & \cdots c_n\end{pmatrix} \tag{1.44}$$

是另一个置换,此处 $b_j=j\rho$ 及 $c_j=a_j\rho$. 置换的合成遵循合成映射的规则. 可是,为了简便,我们把乘积写成 $\pi\rho$ 而不写成 $\pi\circ\rho$. 因而 $\pi\rho$ 是一置换,它是由首先实行 π 置换然后实行 ρ 置换的结果. 有些作者采取相反的规定. 当 π 下的 j 的象用 $\pi(j)$ 表示而不是象我们那样用 $j\pi$ 表示时, 相反的规定是更适合的. 当 ρ 象(1.44)所指出的那样,已经对用 π 左乘作好"准备", 乘积 $\pi\rho$ 可以立即写出,即

$$\pi\rho=\begin{pmatrix}1 & 2\cdots n\\ c_1 & c_2\cdots c_n\end{pmatrix},$$

因为对于任一$j(j=1,2,\cdots,n)$，$j\pi=a_j$ 及 $a_j\rho=c_j$，所以 $j\pi\rho=(j\pi)\rho=a_j\rho=c_j$。

例如，当

$$\pi=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix},\quad \rho=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix}$$

时，在 ρ 恰当的重新排列之后，我们看出

$$\pi\rho=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}\begin{pmatrix}2 & 3 & 4 & 1\\ 1 & 2 & 4 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 4 & 3\end{pmatrix}.$$

顺便地提一下，

$$\rho\pi=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix}\begin{pmatrix}3 & 1 & 2 & 4\\ 4 & 2 & 3 & 1\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 3 & 1\end{pmatrix}.$$

这证明置换乘法一般是非交换的*，

置换

$$\iota=\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}=\cdots=\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ a_1 & a_2 & \cdots & a_n\end{pmatrix}$$

使所有的对象不变，它明显地满足关系 $\iota\pi=\pi\iota=\pi$，因而是恒等置换。π 的逆元素用下面的符号给出：

$$\pi^{-1}=\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ 1 & 2 & \cdots & n\end{pmatrix}$$

（在非标准形式下），因为易于验证

$$\pi\pi^{-1}=\pi^{-1}\pi=\iota.$$

例如

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}^{-1}=\begin{pmatrix}2 & 3 & 4 & 1\\ 1 & 2 & 3 & 4\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}.$$

---

* 当采用相反的规定时，乘积 $\pi\rho$ 与 $\rho\pi$ 必须互换.

不需要去验算结合律，因为它已经包括在映射的一般性质内．因此我们证明了下面的定理．

定理 1 关于 n 个对象的所有置换的集 S_n 形成一个 $n!$ 阶的群，称为 n 次对称群，合成规则是这些对象到自身上的映射的合成．

做少许的练习，读者就会习惯于得出两个或更多置换的乘积而不用写出中间步骤．例如，设

$$\alpha=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\quad \beta=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},$$

$$\gamma=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}.$$

为了得出乘积 $\alpha\beta\gamma$，我们依次考查当置换 α,β,γ 相继实行时，每一个对象所经过的变化．因而

$$1\to2\to1\to4$$
$$2\to3\to2\to3$$
$$3\to1\to4\to1$$
$$4\to4\to3\to2,$$

此处每一行中箭头表示 α,β 与 γ 的作用(按这次序)，且从左向右念．所以

$$\alpha\beta\gamma=\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}.$$

作为进一步的实例，我们列举 S_3 的 6 个置换：

$$\left.\begin{array}{lll}\iota=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, & \alpha=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, & \beta=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\\ \gamma=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, & \delta=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, & \varepsilon=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\end{array}\right\} \quad (1.45)$$

审查一下群 S_3 的结构，我们认出 S_3 是与前面表(v)所表示的抽象群同构的．这同构是通过将 ι 与 1 配对，将希腊字母与相应的

拉丁字母配对而建立的．例如，根据置换相乘的法则，我们看出

$$\alpha\gamma=\varepsilon,\quad \beta\gamma=\delta,$$

它们对应表(v)中的关系

$$ac=e,\quad bc=d.$$

因而我们又得到这个抽象群的另一种表示．

设集Σ分成两个互不相交的子集，比如说

$$\Sigma_1=\{1,2,\cdots,m\},\quad \Sigma_2=\{m+1,m+2,\cdots,n\}.$$

又设π与ρ是Σ的这种置换，使得π只作用在Σ_1上，而让Σ_2的每一个对象不变，ρ只作用在Σ_2上而不变Σ_1的任一个对象．那么很明显$\pi\rho=\rho\pi$，因为π与ρ的作用互不干扰．因而我们注意到，作用在互不相交的对象集上的置换互相交换．

循环地交换m个对象的置换称为m次轮换．因而假如对象用$1,2,\cdots,m$表示，这置换使用下面的符号表示

$$\gamma=\begin{pmatrix}1 & 2 & \cdots & m-1 & m\\ 2 & 3 & \cdots & m & 1\end{pmatrix}. \tag{1.46}$$

假如我们想象m个对象安放在圆周的m个位置上，那么γ移动每一个对象到下一个位置，因此，特别，最后的对象就占有第一个位置．通常将轮换写成缩写符号

$$\gamma=(1,2,\cdots,m),$$

认为它等价于(1.46)．因此

$$\left.\begin{aligned} i\gamma&=i+1\quad(i=1,2,\cdots,m-1),\\ m\gamma&=1.\end{aligned}\right\} \tag{1.47}$$

因为无论从哪一个对象开始运算都没有关系，所以我们能够用下面任一个等价的形式表示γ：

$$\begin{aligned}(1\quad 2\quad \cdots\quad m)&=(2\quad 3\quad \cdots\quad m\quad 1)=\cdots\\ &=(m\quad 1\quad \cdots\quad m-1).\end{aligned}$$

γ的作用能用方程(1.47)描写，或者更简单地用

$$j\gamma=j+1\ (\mathrm{mod}\ m) \tag{1.47$'$}$$

描写，(1.47)′的右边理解为约化成模 m 的最小正剩余．类似地，γ 的 r 次幂的作用总结为

$$j\gamma^r = j + r (\mathrm{mod}\ m). \tag{1.48}$$

因此很明显 $\gamma^m = \iota$，而 $\gamma^r \neq \iota$，当 $0 < r < m$ 时．因而我们看出 m 次轮换是 m 阶的．

今后，我们约定在置换 π 下固定不变的对象无需明显地在 π 的符号中写出．例如，当 $n = 3$ 时，

$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

而当 $n = 5$ 时，

$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}.$$

严格地讲，符号 $(1\ 2\ 3)$ 在此处表示两个不相同的置换，各自具有不相同的次数．但是根据上下文，涉及多少对象，因而哪些对象不变一般是清楚的．

将一置换表示为一些轮换的乘积通常是方便的，这些轮换分别作用在不相交的对象集上．比如，当 $n = 7$ 时，

$$\pi = (1\ \ 2)(4\ \ 6\ \ 7)$$

表示置换

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 7 & 4 \end{pmatrix}.$$

不论什么置换都可以分解成互不相交的轮换．为了说明这一点，我们引入 π 下的轨道的概念．选取任一对象 p，看重复应用 π 之后对 p 会发生什么影响．集

$$p, p\pi, p\pi^2, \cdots \tag{1.49}$$

称为 p 的轨道．因为(1.49)中的对象不能全都不同，一定有非负整数 r, s，使得 $s > r$ 而且 $p\pi^s = p\pi^r$．因而 $p\pi^{s-r} = p$．因此存在一个最小正整数 h，使得

$$p\pi^h = p. \tag{1.50}$$

于是很清楚，π 包含 h 阶轮换

$$(p\ p\pi\ p\pi^2\ \cdots\ p\pi^{h-1}). \tag{1.51}$$

假如 q 是任一不包含在(1.51)中的对象，那么，设 k 是使得 $q\pi^k = q$ 的最小正整数. 因而 q 生成轮换

$$(q\ q\pi\ q\pi^2\ \cdots\ q\pi^{k-1}). \tag{1.52}$$

重要的是注意轮换(1.51)与(1.52)没有公共元素，因为假设

$$p\pi^a = q\pi^b,$$

那么

$$q = p\pi^{a-b}.$$

用 h 除 $a-b$，我们得到

$$a-b = th + r,$$

此处 $0 \leqslant r < h$. 因而就有

$$q = p\pi^r.$$

这与 q 的选择矛盾. 假如有一个对象不包含在(1.51)与(1.52)内，这对象将生成另外的轮换，它与前面的轮换不相交. 我们如此继续建立轮换，一直到所有的对象都包括为止. 在 π 下保持不变的对象生成一个长度为 1 的轮换，根据我们的约定，它可以省去. 用更专门的术语，我们可以说在 Σ 的对象之间已经建立了一个等价关系，两个对象是等价的，当且仅当它们属于同一轨道因而属于同一轮换. 象读者将要知道的那样，Σ 上的一个等价关系总是导致将 Σ 分成不相交的等价类的一个划分. 在目前，这些等价类相当于 π 的轮换因子. 因此我们已经证明了下面的定理.

定理 2　*一个置换可以分解成互不相交的轮换的乘积. 这些轮换互相交换，而且除开这些轮换因子重新排列之外，这分解是唯一的.*

例　设

$$\pi=\begin{pmatrix}1&2&3&4&5&6&7&8\\4&5&6&1&7&8&2&3\end{pmatrix}.$$

从对象 1 开始，我们看出它的轨道是 1，4. 因而 π 包含轮换 (1　4). 对于任一不在这轮换内的对象，比如说 2，我们继续去找它的轨道，得到 2 的轨道 2,5,7，它给出轮换 (2　5　7). 最后我们得到轨道 3,6,8，因而得到轮换 (3　6　8). 因为不再有对象需要考虑，所以我们证明了

$$\pi=(1\ 4)(2\ 5\ 7)(3\ 6\ 8)$$

习　题

(1) 证明下面各数集对于通常的乘法形成无限阿贝尔群。

(a) $\{2^k\}(k=0,\pm1,\pm2,\cdots)$,

(b) $\left\{\dfrac{1+2m}{1+2n}\right\}$ $(m,n=0,\pm1,\pm2,\cdots)$,

(c) $\{\cos\theta+i\sin\theta\}$，此处 θ 遍历所有有理数。

(2) 当 a 与 b 的合成规则规定为 a/b 时，为什么正有理数不能形成一个群？

(3) 设 a 是一映射 $x\to\alpha x+\beta$，此处 α 与 β 是给定的复数，而 $\alpha\neq1$. 试对 a^n 求出一公式，此处 n 是一正整数. 且证明 a 是有限阶的当且仅当 α 是一个单位根.

在习题(4)到(8)中假设元素位于一群中，因此结合律是不成问题的。

(4) 假如 a,b 与 ab 都是 2 阶元素，证明 a 与 b 交换。

(5) 证明元素 ab 与 ba 具有相同的阶。

(6) 假如 $ba=a^mb^n$，证明元素 a^mb^{n-2}，$a^{m-2}b^n$ 与 ab^{-1} 具有相同的阶。

(7) 假如 $b^{-1}ab=a^k$，证明 $b^{-r}a^sb^r=a^{sk^r}$。

(8) 设 x 是 mn 阶元素，此处 $(m,n)=1$. 证明 x 能表示成 $x=yz$，此处 y 与 z 交换，而且分别是 m 阶与 n 阶的元素。

(9) 证明偶阶群包含奇数个 2 阶元素。

(10) 在模 7 剩余类 1,2,3,4,5,6 的乘法群中，求出每个元素的阶，并证明这个群是 6 阶循环群。

（11）证明矩阵

$$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix},\ \begin{bmatrix}\omega & 0\\0 & \omega^2\end{bmatrix},\ \begin{bmatrix}\omega^2 & 0\\0 & \omega\end{bmatrix},\ \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix},\ \begin{bmatrix}0 & \omega^2\\\omega & 0\end{bmatrix},\ \begin{bmatrix}0 & \omega\\\omega^2 & 0\end{bmatrix}$$

$$(\omega^3=1,\ \omega\neq 1)$$

对于矩阵乘法形成一个 6 阶的群. 证明这个群与表（v）所给出的群是同构的.

（12）证明扩充的 z-平面到自身上的映射

$$f_1:\ z\to z,\ f_2: z\to -z,\ f_3: z\to\frac{1}{z},\ f_4: z\to\frac{-1}{z}$$

形成一个群，它与表(iii)所给出的群是同构的.

（13）分解

$$(\mathrm{i})\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3\end{pmatrix}\text{与}$$

$$(\mathrm{ii})\begin{pmatrix}a & b & c & d & e & f\\c & e & d & f & b & a\end{pmatrix}$$

成为互不相交的轮换的乘积，并求出这两个置换的阶。

（14）用互不相交的轮换来表示以下各置换：

(i) $(a\ b\ c\ \cdots k)(a\ l)$；

(ii) $(a_1a_2\cdots a_rxyb_1b_2\cdots b_s)(a_ra_{r-1}\cdots a_1xyc_1c_2\cdots c_t)$；

(iii) $(a_1a_2\cdots a_rxyzb_1b_2\cdots b_s)(a_ra_{r-1}\cdots a_1xyzc_1c_2\cdots c_t)$。

（15）验证置换

$$\iota(\text{恒等置换}),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),$$
$$(1\ 4)(2\ 3)$$

形成一个 4 阶阿贝尔群，且与表(iii)所给出的群同构。

（16）证明矩阵集合

$$A(v)=\left(1-\frac{v^2}{c^2}\right)^{-\frac{1}{2}}\begin{bmatrix}1 & -v\\-v/c^2 & 1\end{bmatrix},$$

此处 c 是一个正常数，v 在区间 $-c<v<c$ 内变化，对于合成规则

$$A(v_1)A(v_2)=A(v_3),$$

$$v_3=\frac{v_1+v_2}{1+\frac{v_1+v_2}{c^2}},$$

形成一个群(罗伦兹群)。

第二章　子　　群

§ 8. 子集. 因为群G是元素的集合，所以集论中通常的定义和符号可以应用到G上. 因而，假如$A, B, C, \cdots$是G的子集，我们用$A \subset B$来表示A的每一元素也是B的元素，包括A与B相等的可能情况.并集$A \cup B$是这样一些元素的集，它们或者属于A或者属于B，或者同时属于A与B. 交集$A \cap B$由同时属于A与B的元素组成；假如不存在这样的元素，我们写$A \cap B = \varnothing$(空集). 记号$a \in A$表示元素a属于A. 在有些地方我们采用这种约定（稍有些不合逻辑）：将元素a等同于只包含单个元素的集. 因而假如A的元素是$a_1, a_2, a_3, \cdots$，我们将写成

$$A = a_1 \cup a_2 \cup a_3 \cup \cdots$$

G中所定义的乘法给予G的子集间一个附加的结构. 给定任意两个子集A与B，我们规定

$$AB \tag{2.1}$$

为所有能以形式ab表示的元素的集，此处$a \in A$及$b \in B$. 这些乘积不一定彼此不同，因为可能$a_1 \neq a_2, b_1 \neq b_2$，但是$a_1 b_1 = a_2 b_2$. 可是我们强调$AB$只被当作一个集合，因此其中元素的重现不予考虑. 象平常一样，子集是相等的当且仅当它们包含同样的不同元素. 以后，子集间的相等总是按以上的意义去理解. 当然，一般

$$AB \neq BA.$$

但是即使$AB = BA$，这一等式并不意味A的每一元素与B的每一元素交换. 我们只能够推断，对于任一$a \in A$及任一$b \in B$，存在元素$a' \in A$及$b' \in B$，使得$ab = b'a'$.

容易验证子集的乘法是结合的，即

$$(AB)C = A(BC). \tag{2.2}$$

因此(2.2)式的每边可以简单地以 ABC 表示. 用一个明瞭的缩写，我们令

$$A^2=AA, \qquad A^3=AAA, \cdots$$

因而 A^2 是能用 a_1a_2 的形式表示的元素的集合，此处 a_1 与 a_2 遍历 A.

容易建立下面的法则：

$$(A\cup B)C=AC\cup BC,$$
$$C(A\cup B)=CA\cup CB,$$
$$(A\cap B)C=AC\cap BC,$$
$$C(A\cap B)=CA\cap CB.$$

我们注意某些集只包含单独一个元素这种特殊情况. 因而假如 x 与 y 是 G 的元素，那么 Ax 是所有形为 ax 的元素的集，yAx 由所有 yax 的元素组成，此处 a 遍历 A. 我们看到

$$x^{-1}(A_1\cap A_2\cap\cdots\cap A_r)x$$
$$=x^{-1}A_1x\cap x^{-1}A_2x\cap\cdots\cap x^{-1}A_rx. \qquad (2.3)$$

当 G 是阿贝尔加法群时，两个集 A 与 B 的合成写为

$$A+B,$$

它是所有能以 $a+b$ 的形式表示的元素的集，此处 $a\in A$ 及 $b\in B$. 特别，子集

$$A+A$$

(它不能简略为 2 A 见§ 2)是所有元素 $a+a'$ 的集合，此处 a 与 a' 属于 A. 当 x 是 G 的一个固定元素时，子集

$$A+x$$

由元素 $a+x(a\in A)$ 组成，对于 $A+(-x)$，我们用记号 $A-x$ 表示.

一般来说，消去律不适用于子集的乘法，即，假如 $AC=BC$，我们不能推导出 $A=B$. 但是 $Ax=Bx$ 蕴含 $A=B$，而 $Ax=C$ 等价于 $A=Cx^{-1}$. 相似的结果适用于单独一个元素乘一个集. 在下一章

我们将遇到一个重要的情况，即

$$Ax=xA \quad 或 \quad x^{-1}Ax=A. \tag{2.4}$$

(2.4)意味对每一 $a\in A$ 存在一个元素 $a'\in A$ 使得 $ax=xa'$.

A 的**基数**，即 A 中不同元素的个数，不论是有限或无限，常常用 $|A|$ 表示.

§ 9. **子群**. 我们特别对群 G 的服从群的公设的那些子集感兴趣，这样的子集称为 G 的**子群**. 因而，当 H 满足下面的条件时，H 是 G 的子群：

(1) 假如 $u\in H$，$v\in H$，那么 $uv\in H$（封闭）.

(2) $1\in H$，此处 1 是 G 的单位元素（单位元素）.

(3) 假如 $u\in H$，那么 $u^{-1}\in H$（逆元素）.

我们没有提到结合律，因为它的有效性在整个 G 中是认为不成问题的.

当 H 是 G 的子群时我们往往写成

$$H\leqslant G$$

而不写成 $H\subset G$，符号 $\leqslant$ 只用于子集是群的情形. 我们将用 $<$ 表示严格包含. 假如 H 是一个子群，s 是它的一个元素，那么 H 的封闭性意味 $Hs\subset H$. 另一方面，H 的任一元素 u 总可以写为 $u=(us^{-1})s$. 因为 $us^{-1}\in H$，这证明 $u\in Hs$，所以 $H\subset Hs$，因此

$$Hs=H. \tag{2.5}$$

可以同样地证明

$$sH=H. \tag{2.5$'$}$$

相反地，设 s 是 G 的一元素满足(2.5). 那么，特别，

$$s=1\,s\in H.$$

因此 (2.5) 或 (2.5)$'$ 是 G 中一元素属于子群 H 的必要和充分条件.

读者可以验证这些讨论易于推广，因此我们可以陈述下面的

结果：

命题 3 G的子集S属于子群H，当且仅当

$$HS=SH=H.$$

特别，当 $S=H$ 时，我们得出

$$H^2=H. \tag{2.6}$$

看到这一点是有趣的，即当H是有限集合时，关系式(2.6)反过来意味H是一个群.

命题 4 假如H是G的有限子集，那么H是一子群当且仅当$H^2=H$.

证明 只需证明(2.6)意味H是一个子群. 设H的元素列举如下

$$H: u_1, u_2, u_3, \cdots, u_h. \tag{2.7}$$

设 u 是其中任一元素，那么 h 个元素

$$Hu: u_1u, u_2u, u_3u, \cdots, u_hu \tag{2.8}$$

全都属于H^2，因而根据我们的假设，全都在H内. 此外，这些元素都不相同因为消去律适用于G. 因而集(2.7)与(2.8)除其中元素排列的次序可能不同外是全同的. 特别，元素u必然出现在(2.8)中，因而一定存在一个整数 j 使得

$$u_ju=u,$$

从而 $u_j=1\in H$. 最后，存在一个整数 k 使得

$$u_ku=1(=u_j),$$

即 $u_k=u^{-1}\in H$. 这便证明了H是一个群.

当H是G的(有限或无限的)子群，x 是G的任一元素，那么子集

$$H'=x^{-1}Hx \tag{2.9}$$

也是G的一个子群. 因为假如$x^{-1}ux$与$x^{-1}vx$是H'的任意两个元素，此处$u,v\in H$，那么$(x^{-1}ux)(x^{-1}vx)=x^{-1}uvx\in H'$，还有$x^{-1}1x=1\in H'$及$x^{-1}u^{-1}x=(x^{-1}ux)^{-1}\in H'$. 进一步这两个子群

是同构的，因为

$$u\theta=x^{-1}ux \quad (u\in H)$$

是一个H到H'上的一一映射，而且具有性质

$$(u\theta)(v\theta)=(uv)\theta.$$

因此

$$H\cong H'.$$

我们注意，每一个群G显然具有子群$H=\{1\}$及$H=G$. 位于这两个极端之间的子群称为**真子群**.

§ 10. 陪集. 设H是G的子群，x 是G的任一元素，那么

$$Hx$$

称为G对于H的右陪集，或者更精确地说，由x生成的右陪集或者包含x的右陪集. 因为很清楚，由于$1\in H$，故$x\in Hx$. 当$x=u$时，此处u是H的元素，那么由命题 3，$Hu=H$. 这表示H本身是一个陪集，它可以写成$H1$或者更一般地写成Hu，此处u是H的任一元素.

从这些讨论中可以看到，两个不同元素可以生成同一个陪集. 现在让我们求出使得

$$Hx=Hy \tag{2.10}$$

的必要和充分条件，此处x与y是G的元素. 假如(2.10)正确，那么，特别地，$x=1x\in Hy$，因此存在元素$u\in H$，使得

$$x=uy$$

或

$$xy^{-1}\in H. \tag{2.11}$$

相反地，假如(2.11)成立，那么

$$Hx=Huy=Hy.$$

任意两个陪集或者全同或者没有公共元素，换句话说，假如两个陪集具有一个公共元素，那么它们就全同. 因为假设

$$z\in Hx\cap Hy,$$

那么存在H的元素u与v使得

$$z=ux=vy,$$

因而

$$xy^{-1}=u^{-1}v\in H,$$

这意味$Hx=Hy$. 我们把这些结果总结在下面的命题中.

命题 5 设H是群G的子群,那么陪集Hx与Hy是全同的当且仅当$xy^{-1}\in H$. 任意两个陪集或者全同或者没有公共元素.

值得以更抽象的观点观察一下这种情况. 我们说两个元素x, $y\in G$是等价的(对于H),写成$x\sim y$,假如存在一个元素$u\in H$使得$x=uy$,或者等价地说,假如

$$Hx=Hy,$$

即假如x与y位于H的同一右陪集内. 很清楚,事实上这的确定义了一个等价关系. 因为(i)$x\sim x$,(ii)$x\sim y$意味$y\sim x$,(iii)假如$x\sim y$及$y\sim z$,那么x,y与z都位于同一陪集中,因此$x\sim z$.

一般地说,当某一个等价关系已经在某一个集上规定,这个集就可以表示成不相交子集的并集, 即所有不同的等价类的并集. 在目前情况中, 等价类是右陪集, 所以G是所有不同的陪集的并集. 为了更正式地表示这个结果, 我们从每一陪集中选择一个代表. 假如t_i是其中一个代表,对应的陪集可以表示为Ht_i. 不同右陪集的集合可能是无限的甚至是不可数的. 在这种情况下我们用一个指标集I来描写, 它的元素与陪集一一对应. G是所有不同陪集的并集这件事因而可用公式表为

$$G=\bigcup_{i\in I}Ht_i, \tag{2.12}$$

不同的右陪集的个数,即I的基数, 称为H在G中的**指数**, 表示为

$$[G:H]. \tag{2.13}$$

当存在无限多右陪集时,我们令$[G:H]=\infty$.

这些代表的集合$\{t_i, i\in I\}$称为H在G中的**右横截**. 虽然H在

G 中的指数完全由 H 与 G 决定，但横截明显地不是唯一的，假如知道一个横截$\{t_i, i\in I\}$，最一般的横截就是

$$\{u_i t_i; i\in I\},$$

此处 u_i 是 H 的任一元素.

用类似的方法我们可以考虑 H 的**左陪集**. 标准的左陪集是 $xH(x\in G)$，容易验证，

$$xH=yH$$

当且仅当存在一个元素 $v\in H$ 使得 $x=yv$，或当且仅当

$$y^{-1}x\in H. \tag{2.14}$$

象前面一样，两个左陪集或者全同或者没有公共元素，于是 G 可以分划成所有不同的左陪集的不相交并集，因而

$$G=\bigcup_{j\in J} s_j H,$$

此处 J 是列举左陪集的指标集，而$\{s_j\}$是左陪集的代表集. 或者，象我们将要说的那样，$\{s_j\}$是 H 在 G 中的左横截，不过容易看出指标集 I 与 J 具有相同的基数. 事实上，从分解式(2.12)出发我们将证明

$$G=\bigcup_{i\in I} t_i^{-1}H \tag{2.15}$$

是 G 的左陪集分解式. 首先我们看出(2.15)中的陪集彼此不相同，因为假如

$$t_i^{-1}H=t_k^{-1}H,$$

那么

$$(t_k^{-1})^{-1}t_i^{-1}\in H,\quad t_k t_i^{-1}\in H,$$

因而 $Ht_k=Ht_i$，这是不可能的，除非 $i=k$. 其次，每一元素 $x\in G$ 包含在(2.15)右边的并集中，因为 x^{-1} 一定在分解式(2.12)的某一个右陪集中，比如说 $x^{-1}\in Ht_m$，因而 $x\in t_m^{-1}H$，这证明了(2.15)，同时我们也证明了左陪集可用与右陪集相同的指标集来

列举．我们记住H是一陪集（左陪集或右陪集）．当H是有限时，象在(2.7)中那样，Ht的元素是

$$u_1t, u_2t, \cdots, u_ht.$$

因此每一陪集包含h个元素．

我们现在能够证明关于有限群的最古老和最重要的定理之一．

定理 3（拉格朗日 Lagrange）　设G是g阶有限群，假如H是h阶的子群，那么

(i) h除尽g，即$g=nh$及

(ii) n等于指数$[G:H]$，因此分别存在G的右陪集和左陪集分解式

$$G=\bigcup_{i=1}^{n} Ht_i,\ G=\bigcup_{i=1}^{n} s_iH. \tag{2.16}$$

证明　分解式(2.16)的存在已经在一般的情况下证明过，此处n是指数．我们只需证明

$$g=nh.$$

计算一个分解式两边元素的个数就可以立即得出这结果．因为我们已经知道每一陪集包含h个元素，而G是n个不相交陪集的并集，这就说明了G的全部元素数$g=nh$．

推论 1　如果G是g阶有限群，则G的每一元素的阶是g的某一因子．G的所有元素满足方程

$$x^g=1.$$

证明　设u是G的元素，因为G是有限的，元素u的阶一定也是有限的，比如说阶是r，因而元素

$$1, u, u^2, \cdots, u^{r-1}(u^r=1)$$

形成一个r阶循环子群．由拉格朗日定理，r能除尽g，因此$g=sr$，此处s是正整数，因此

$$u^g=(u^r)^s=1.$$

推论 2　素数阶的群没有真子群，因而必然是循环群.

证明　设 G 是一个 p 阶群，此处 p 是素数. 任一子群的阶或者是 1 或者是 p，即这子群或者只包含单位元素或者与 G 同阶.

假如 u 是 G 的任一非单位元素，那么 u 的阶大于 1 而且是 p 的一个因子. 因而 u 是 p 阶，这些元素

$$1, u, u^2, \cdots, u^{p-1}$$

是不同的，因而是 G 的全部元素.

例　§4 表(v)中给出的 6 阶的群中，a,b,c,d,e 的阶分别是 3,3,2,2,2.

当 G 是加法阿贝尔群且 H 是 G 的子群时，H 的标准陪集写为

$$H+x.$$

我们有

$$H+x=H+y$$

当且仅当

$$x-y\in H,$$

或者说

$$x=y+u,$$

此处 u 是 H 的一个元素. 在这情况中，我们有时说 x 与 y 模 H 同余，写为

$$x\equiv y \pmod H.$$

§ 11. 循环群的子群. 首先考虑无限循环群的情况

$$C: 1(=x^0), x, x^{-1}, x^2, x^{-2}, \cdots \tag{2.17}$$

不考虑平凡子群{1}，我们可以说 C 的每一个子群 H 由 x 的某些幂组成，包括 1 在内，因而

$$H: 1, x^a, x^b, \cdots,$$

此处 $a, b, \cdots$ 是正整数或负整数. 因为当 x^a 属于 H 时，x^{-a} 也属于 H，那么 C 的每一个非平凡子群至少包含 x 的一个具有正指数

的幂，因而H中存中一个x的幂具有最小的正指数，比如说x^m. 因此，H包含所有下面这样形式的元素

$$x^{mq}(q=0,\pm 1,\pm 2,\cdots), \tag{2.18}$$

即H包含由x^m生成的循环群. 我们断定除列举在(2.18)中的元素外，H中不存在别的元素. 因为设x^a是H的任一元素，用m除a，因而有

$$a=mq+r,$$

此处$0\leqslant r<m$，因此

$$x^a=x^{mq}x^r,$$

$$x^a x^{-mq}=x^r.$$

既然左边的两个因子都属于H，那么x^r也是H的一个元素. 但是这与m的最小性相矛盾，除非$r=0$. 因而$a=mq$，即(2.18)包含H的全部元素. 我们看出无限循环群C的每一非平凡子群本身也是一个无限循环群，因而与C同构.

当我们讨论有限循环群的子群时就更有趣了，有关结论总结在下面的定理中.

定理 4 设

$$C:1,x,x^2,\cdots,x^{g-1}(x^g=1) \tag{2.19}$$

是g阶循环群. 那么对应每一个g的因子h，存在且仅存在一个h阶的子群，它可以由$x^{g/h}$生成.

证明 (i) 设$g=hn$，元素

$$1,x^n,x^{2n},\cdots,x^{(h-1)n} \tag{2.20}$$

是不同的，因为它们间的等式会导致关系式

$$x^{ln}=1,$$

此处

$$0<ln<hn(=g),$$

与x是g阶元素相矛盾. 因此(2.20)形成一个h阶的子群，它由h阶元素x^n生成. (ii) 反之，假设$h\mid g$，比如说$g=hn$，而

$$H:1,u_2,u_3,\cdots,u_{h-1}$$

是一个 h 阶的子群，每一个 u_i 是 x 的一个幂，比如说

$$u_i=x^{\lambda_i},(i=2,3,\cdots,h-1),$$

此处 λ_i 是一整数满足

$$0<\lambda_i<g.$$

因为 H 是 h 阶的，推论 1 意味

$$u_i^h=1,$$

即
$$x^{h\lambda_i}=1.$$

由本定理的假设，$x^g=1$，于是 $g\mid h\lambda_i$. 因而存在整数 k_i 使得

$$h\lambda_i=k_ig=k_ihn,$$

$$\lambda_i=k_in.$$

这证明了 H 的每一元素是 x^n 的幂. 只有 h 个这样的幂不相同，它们列举在(2.20)中. 因而 H 是(2.20)的子集，但 H 是 h 阶的，它必然与(2.20)给出的集全同，这证明了后者是唯一的h阶子群.

§ 12. 交集与生成元. 通过研究子群常能阐明群的结构. 因此掌握构造子群的方法是重要的.

很清楚，假如 $H\leqslant G$ 及 $K\leqslant H$，那么 $K\leqslant G$. 其次，假如 H 与 K 是 G 的子群，那么它们的交集

$$D=H\cap K$$

也是 G 的子群，因为假如 x 与 y 属于 D，我们有 $x,\ y\in H$ 及 $x,\ y\in K$，从而 $xy\in H$，$xy\in K$，即 $xy\in D$；也有 $1\in D$，因为 $1\in H$ 及 $1\in K$；最后假如 $x\in D$，那么 $x^{-1}\in H$，$x^{-1}\in K$，因此 $x^{-1}\in D$. 这证明了 D 是一个子群，更一般地说，任意多个子群的交集

$$H\cap K\cap L\cdots$$

是一个子群.

另一方面，两个子群的并集

$$H\cup K$$

一般不是子群. 因为假如 $u\in H$ 及 $v\in K$，没有理由假设 uv 属于

H 或者属于 K，从而 uv 在 $H \cup K$ 中. 为了得出包含 H 与 K 的最小子群，需要一个更精致的构造方法.

设

$$a, b, c, \cdots \tag{2.21}$$

是 G 的元素的集合，考虑所有包含有限个因子乘积的集，这些因子可能重复，它们从(2.21)的元素中或者从(2.21)元素的逆元素中选出，例如 $a^2b^{-1}cab$. 在这些乘积中我们包括"空"积，它与 G 的单位元素等同. 很明显，这些乘积的集形成一个群，因为假如我们将两个含有有限个因子的积相乘我们得出另外一个同样类型的乘积，且这些乘积的逆也属于这个集. 用这样方法构成的群表示为

$$\mathrm{gp}\{a, b, c, \cdots\} = M, \tag{2.22}$$

称为由 $a, b, c, \cdots$ 生成的群. 很明显，每一个包含(2.21)中的元素的群必然包含 M，这证实了 M 是包含这些元素的最小子群. 换句话说，我们可以说 M 是所有包含(2.21)中的元素的群的交集. 自然，可能发生 $M = G$.

元素 $a, b, c, \cdots$ 称为 M 的**生成元**. 不过应该指出，生成元不是唯一的，一般也不假定它们是没有多余的. 例如，如果生成元

$$a \in \mathrm{gp}\{b, c, \cdots\},$$

则 a 是多余的. 在这情况下我们用下式代替(2.22)

$$M = \mathrm{gp}\{b, c, \cdots\}.$$

我们主要对有限生成群感兴趣. 很明显这样的群总具有一组不多余的生成元. 因为事实上我们可以从任一个生成元集出发，然后消去那些可以用其他生成元表示的生成元.

每一个群 G 总能表成(2.22)的形式，例如我们可以把所有 G 的元素当作生成元，然后假如需要就去掉多余的生成元. 就实际应用来说，要求尽可能地减少生成元的个数.

只有一个生成元 x 的群是由 x 生成的循环群，可以写为 $\text{gp}\{x\}$. 为了说明这个概念，让我们再一次回到6阶群 $G(\cong S_3)$，它在§4中用表(v)表示. 我们发现六个元素都能用 a 与 c 表示如下

$$1=c^2=(a^3),a=a,b=a^2,$$
$$c=c,d=ca,e=ca^2. \tag{2.23}$$

因而在这情况中我们写成

$$G=\text{gp}\{a,c\}. \tag{2.24}$$

另外，可以证明

$$G=\text{gp}\{b,d\}. \tag{2.25}$$

因为 a 与 c，因而整个群，能用 b 与 d 表出，即

$$a=b^2, \quad c=db.$$

在(2.24)或(2.25)中的生成元肯定没有多余的，因为这个群是非阿贝尔群因而不能用单独一个元素生成，假如它由单独一个元素生成，那么它将是循环的，因而是阿贝尔群.

认识到不多余的生成元仍然可以用非平凡的关系式联系起来是重要的. 比如查阅表(v)，我们发现

$$ac=ca^2, \tag{2.26}$$

它等价于

$$(ac)^2=1, \tag{2.26$'$}$$

因为 $(ac)^2=acac=acca^2=a\,1\,a^2=a^3=1$. 不可能解出任何一个这样的方程使得某一生成元可以用其他的生成元表示. 象(2.26)或(2.26)′那样的方程式称为定义关系. 用一组生成元和一组定义关系来指定一个特殊的群常常是方便的. 我们以后还要回来更详细地说明这一原则(第五章). 在目前情况下我们只说明方程

$$a^3=c^2=(ac)^2=1 \tag{2.27}$$

可以作为一组定义关系. 的确，包含在(2.27)中的知识足以构造

整个乘法表. 首先,我们注意到六个元素

$$1,a,a^2,c,ca,ca^2 \qquad (2.28)$$

肯定是不相同的. 例如假如 a 等于 ca^2,那么 $a^{-1}=c$, 这与 a 和 c 是不多余的生成元这一事实相矛盾. 其次, 我们利用 (2.27)来验证(2.28)对乘法是封闭的. 例如

$$(ca)(ca^2)=c(ac)a^2=cca^2a^2=c^2a^4=a,$$

$$a^2c=a(ac)=aca^2=ca^4=ca,$$

等等,这里利用(2.26),将因子 c 有规律地移到左边, 直到乘积与(2.28)中的某一个元素相同为止. 在这种记号下完整的乘法表如下:

(Vii)	1	a	a^2	c	ca	ca^2
1	1	a	a^2	c	ca	ca^2
a	a	a^2	1	ca^2	c	ca
a^2	a^2	1	a	ca	ca^2	c
c	c	ca	ca^2	1	a	a^2
ca	ca	ca^2	c	a^2	1	a
ca^2	ca^2	c	ca	a	a^2	1

它还提供了首先在 §4 表(v)中所呈现的那个群的另一种表示方法.

假如 $A, B, C, \cdots$ 是群 G 的子集, 由它们所生成的群表示为

$$\mathrm{gp}\{A,B,C,\cdots\},$$

它定义为全部有限乘积的集合,在这些乘积中每个因子是 A 或 B 或 $C\cdots$ 的元素或这样的元素的逆,它们在乘积中按任一次序排列并且可以重复. 假如我们把所有 $A\cup B\cup C\cup\cdots$ 的元素当作生成元,这就归结到先前的生成元的概念. 因而我们同样可以写为

$$\mathrm{gp}\{A\cup B\cup C\cup\cdots\}.$$

当然,假如 A 是子群,我们有 $A=\mathrm{gp}\{A\}$.

§ 13. 直积. 我们现在来讨论由两个群构造出一个新的群的简单

方法. 设 H 与 K 是任意群,考虑所有对

$$(u,v)$$

的集,此处 u 与 v 分别遍历 H 与 K. 这些对的集表示成

$$G=H\times K,$$

称为 H 与 K 的**(外)直积**. 集 G 由于赋予它下面的合成规则而成为群

$$(u,v)(u',v')=(uu',vv'). \tag{2.29}$$

容易证明结合律适用于 G, 因为乘法在 H 中与 K 中是结合的. G 中单位元素是对

$$(1_H,1_K),$$

此处 1_H 与 1_K 分别是 H 与 K 中的单位元素. 还有

$$(u,v)^{-1}=(u^{-1},v^{-1}).$$

假如 H 与 K 分别是 h 阶与 k 阶的有限群,那么 $H\times K$ 是 hk 阶的群.

更一般地说,假如 $H_1,H_2,\cdots,H_r$ 是任意群, 它们的直积

$$H_1\times H_2\times\cdots\times H_r$$

由所有 r 重元素

$$(u_1,u_2,\cdots,u_r)$$

构成,此处 $u_i\in H_i(i=1,2,\cdots,r)$, 而乘法就在 r 重元素的每一分量中实行. 假如每一 H_i 是有限的,那么显然

$$|H_1\times H_1\times\cdots\times H_r|=\prod_{i=1}^{r}|H_i|.$$

有时碰巧群 G 与它的两个子群 H 与 K 的直积同构,

$$G\cong H\times K, \tag{2.30}$$

或者稍微滥用一下记号

$$G=H\times K. \tag{2.30$'$}$$

这是在下面的情况下而发生的:

(1) 子群 H 的元素与 K 的元素互相交换，即，假如 u 与 v 分别是 H 与 K 的任意元素，那么

$$uv=vu. \tag{2.31}$$

(2) 每一元素 $x\in G$ 能表示成 $x=uv$ 的形式，或者更简单地写成

$$G=HK. \tag{2.32}$$

(3) H 与 K 的交集是单位元素，即

$$H\cap K=1. \tag{2.33}$$

我们注意(2)与(3)等价于单独一个条件：

(2′) 每一元素 $x\in G$ 能唯一地分解为 $x=uv$，此处 $u\in H$ 及 $v\in K$.

因为假设(2)与(3)成立，又假设我们有两个分解

$$x=uv=u_1v_1,$$

那么

$$u_1{}^{-1}u=v_1v^{-1}. \tag{2.34}$$

而(2.34)两边的元素各属于 H 和 K，从而，由(3)它必然等于 1，因此 $u=u_1$ 及 $v=v_1$，这就证明了(2′)所要求的分解的唯一性.

反之，假定(2′)成立及假设 $w\in H\cap K$. 那么 $w=1\ w=w\ 1$ 是 w 的两个因子分别在 H 和 K 中的分解式，从分解的唯一性我们推导出 $w=1$.

以上的条件使我们明白，每一元素 $x\in G$ 唯一地决定对 (u,v)，此处 $u\in H$ 与 $v\in K$，以及每一个这样的对都出现，因为 (u,v) 对应于乘积 $uv=x$. 对应

$$x\theta=(uv)\theta=(u,v)$$

建立同构(2.30)，因为由(1)，

$$(uv)(u'v')\theta=(uu'vv')\theta=(uu',vv').$$

类似地，我们有

$$G\cong H_1\times H_2\times\cdots\times H_r,$$

此处 $H_i(i=1,2,\cdots,r)$ 是 G 的子群，且假如下面的条件被满

足：

(1) 任意两个群 H_i, H_j 的元素互相交换.

(2) G 的每一元素 x 能用以下形式表示

$$x = u_1 u_2 \cdots u_r, \tag{2.35}$$

此处 $u_i \in H_i$.

(3) $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_r = \{1\}$.

或者，代替(2)与(3)，我们有

(2′) 分解式(2.35)是唯一的. 特别，假如

$$u_1 u_2 \cdots u_r = 1,$$

那么由(2′)，

$$u_1 = u_2 = \cdots = u_r = 1,$$

因为 $1 = 11 \cdots 1$ 是 1 的唯一的分解式，

当一个群已经表示为子群的直积，我们称之为**内直积**.

例 与模 15 互素的最小正剩余是

$$1, 2, 4, 7, 8, 11, 13, 14, \tag{2.36}$$

它们形成一个 8 阶的阿贝尔群(见 § 14). 我们将看到它与两个分别由元素 2 与 11 所生成的循环群的直积同构. 事实上，剩余 2 生成 4 阶的循环群，即

$$C_4: 1, 2, 4, 8 (2^4 = 16 \equiv 1 \pmod{15}),$$

相似地，11 生成 2 阶的循环群

$$C_2: 1, 11 (11^2 = 121 \equiv 1 \pmod{15}).$$

既然整个群是阿贝尔群，我们只需要验证条件(2.32)与(2.33). 取所有可能的积我们得到

$$1, 2, 4, 8, 11, 22, 44, 88,$$

关于模 15 约化后成为

$$1, 2, 4, 8, 11, 7, 14, 13,$$

因为这是全部群，所以条件(2)适用，而且我们立即看出

$$C_4 \cap C_2 = \{1\}.$$

这证明这个群是与 $C_4\times C_2$ 同构的.

下面的简单命题,具有某些独特的重要性,将在下一节用到.

命题 6　设 G 是一有限群，它的所有元素满足方程

$$x^2=1, \tag{2.37}$$

即每一个非单位元素都是 2 阶的. 那么 G 与下面形式的阿贝尔群同构

$$C_2\times C_2\times\cdots\times C_2.$$

因而 G 的阶是 2 的幂.

证明　由拉格朗日定理的推论 2,当 G 是 2 阶的(唯一)群时，命题明显是正确的. 因而假设 G 是阶大于 2 的群，设 a 与 b 是不等于 1 的不相同的元素. 根据假设，

$$a^2=b^2=1,$$

所以

$$a=a^{-1}, b=b^{-1}.$$

其次,考虑元素 ab,由(2.37),$(ab)^2=1$,从而

$$ab=(ab)^{-1}=b^{-1}a^{-1}=ba.$$

这证明了 G 是阿贝尔群. 设 $u_1, u_2, \cdots, u_r$ 是 G 的一组不多余的生成元,因为 G 是阿贝尔群,生成元的乘积可以用这样的方式进行整理,使得每一元素可以表成规范形式

$$u_1^{k_1}u_2^{k_2}\cdots u_r^{k_r}. \tag{2.38}$$

但是由于有(2.37),所以(2.38)中的指数可以限制只取 0 与 1. 于是,所有的乘积将是不相同的,因为两个这样的乘积之间的一个等式会导致关系式

$$u_1^{l_1}u_2^{l_2}\cdots u_r^{l_r}=1,$$

此处每一 l_i 或者是 0 或者是 1. 这将使我们能够用另外的生成元来表示某一个生成元，这与生成元是不多余的假设相矛盾. 因此规范形式(2.38)是唯一的，这等于说

$$G=\mathrm{gp}\{u_1\}\times \mathrm{gp}\{u_2\}\times\cdots\times \mathrm{gp}\{u_r\},$$

因而

$$G\cong C_2\times C_2\times\cdots\times C_2(\text{共 } r \text{ 个因子}).$$

§ 14. 一到八阶群的概论. 我们还没有找到成功的方法来构造所有可能的预先指定阶数的抽象群，除少数简单的情形外，我们事先也不知道存在多少个这样的群.

可是，迄今为止我们所叙述的基本方法足以给出全部 1 阶到 8 阶的群，因为素数阶的群已经讨论过(定理 3，推论 2)，所以只需要更详细地讨论阶 g 等于

$$4, 6 \text{ 或 } 8$$

的情况.

存在两个 4 阶的群，它们都是阿贝尔群.

因为假如 $g=4$，不等于 1 的元素只能是 4 阶或 2 阶(见定理 3，推论 1).

(1) 假如 G 包含一个 4 阶元素 a，这元素生成 G；事实上，G 的四个元素是

$$1, a, a^2, a^3 (a^4=1),$$

我们有 $G=C_4$，4 阶循环群.

(2) 其次，假设 G 没有 4 阶元素. 那么所有与 1 不同的元素都是 2 阶的. 我们从命题 6 推断

$$G=C_2\times C_2.$$

因而 G 由两个元素 a 与 b 生成，而 G 的 4 个元素是

$$1, a, b, ab, \tag{2.39}$$

此处

$$a^2=b^2=1, \quad ab=ba. \tag{2.40}$$

这个群称为**四群**(克莱因的"四群")，常以 V 表示.

由于没有别的可能性，我们断定任一四阶群或者与 C_4 同构，或者与 $V(\cong C_2\times C_2)$ 同构. 这些群的乘法表曾经用另外的记号在 § 4 的表(iii)与表(iv)中表示过.

存在两个 6 阶的群，一个是循环群，另一个是非阿贝尔群.

(1) 假如G具有 6 阶元素 a，那么

$$G=\mathrm{gp}\{a\}=C_6.$$

(2) 其次，假设不存在 6 阶元素，那么每一个不等于 1 的元素的阶，是 2 或 3(定理 3，推论 1). 因为G的阶不是 2 的幂，所以不是所有G的元素都能满足(2.37). 因而至少有一个 3 阶元素 a，使得

$$1,a,a^2 \tag{2.41}$$

是G的三个不同元素，而

$$a^3=1. \tag{2.42}$$

假如 c 是G的另外一个元素，则 6 个元素

$$1,a,a^2,c,ca,ca^2 \tag{2.43}$$

是不相同的，象我们对列举在(2.28)中的元素所指出的那样.

假如(2.43)中的元素形成一个 6 阶群，封闭性公理必须满足. 特别，c^2 必然是这些元素中的一个. 我们不能有一个形式为 $c^2=ca^i(i=0,1,2)$的等式，因为这意味 c 属于集(2.41). 所以只剩下下面三种可能性：

$$(\alpha)\ c^2=1,(\beta)\ c^2=a,(\gamma)\ c^2=a^2. \tag{2.44}$$

在(β)与(γ)的假设下，元素 c 不能是 2 阶的，因此必须是 3 阶的. 但是用 c 左乘(β)与(γ)的两边，我们应分别得到 $1=ca$ 及 $1=ca^2$，这两个等式都不正确，因而我们断定(α)必然成立，即

$$c^2=1. \tag{2.45}$$

其次，考虑 ac，它必然是(2.43)中的元素之一. 既然它不能等于 c 或者等于 a 的某一次幂，我们只剩下

$$ac=ca \quad 或者 \quad ac=ca^2 \tag{2.46}$$

两种可能. 头一个等式使得这个群是阿贝尔群. 让我们找出在这情况下 ac 的阶.

$$(ac)^2=a^2c^2=a^2\neq1,(ac)^3=a^3c^3=c^3=c\neq1,$$

所以元素 ac 必然是 6 阶的，这与我们最初的假设不合，因而(2.46)的第二个等式必然成立.
即

$$ac=ca^2 \text{ 或者，等价地，} (ac)^2=1,$$

这一点我们可以参考(2.26)或(2.26)′. 总结以上的讨论我们可以说，假如存在一个 6 阶的群 G 与 C_6 不同，那么

$$G=\mathrm{gp}\{a,c\}$$

服从关系

$$a^3=c^2=(ac)^2=1.$$

这并不证明这样的群存在. 但是我们碰巧知道确实存在这样的群，它的乘法表就在 §12 中. 因此恰好存在两个 6 阶群.

存在五个 8 阶群，三个是阿贝尔群，两个是非阿贝尔群.

三个 8 阶阿贝尔群容易写出，即

(1) $C_8=\mathrm{gp}\{a\}$，此处 $a^8=1$(后面表(viii)).

(2) $C_4\times C_2=\mathrm{gp}\{a\}\times\mathrm{gp}\{b\}$，此处 $a^4=b^2=1$，$ab=ba$(后面表(ix)).

(3) $C_2\times C_2\times C_2=\mathrm{gp}\{a\}\times\mathrm{gp}\{b\}\times\mathrm{gp}\{c\}$，此处 $a^2=b^2=c^2=1, ab=ba, bc=cb, ca=ac$(后面表(x)).

根据我们在第四章将要叙述的一般理论，我们可以说这些群是所有可能的 8 阶阿贝尔群，但是我们将在这里根据前面讨论的原则推导出这个结果. 假如这个群包含一个 8 阶的元素，则它一定是群 C_8，而假如所有与 1 不同的元素都是 2 阶的，那么它与群(3)同构.

因而我们将假定与 1 不同的每一元素或者是 4 阶的或者是 2 阶的，而且至少存在一个 4 阶元素 a，此处

$$a^4=1, \quad a^2\neq 1. \tag{2.47}$$

假如 b 是不含于 $\mathrm{gp}\{a\}$ 中的一元素，那么八个元素

$$1, a, a^2, a^3, b, ab, a^2b, a^3b \tag{2.48}$$

是不相同的，因此构成整个群，假如这样的群存在的话.

于是 b^2 一定是这些元素中的一个，而且事实上一定是前四个元素中的一个，因为 b 不是 a 的幂. 等式 $b^2=a$ 或 $b^2=a^3$ 必须排除，因为它们将意味 b 的阶是 8. 因此还有两种可能性

$$(\alpha)\ b^2=1 \quad 或 \quad (\beta)\ b^2=a^2. \tag{2.49}$$

(α) 假设 $b^2=1$，乘积 ba 一定是(2.48)中最后三个元素之一.

(α,i) 假如 $ba=ab$，这个群是阿贝尔群，它就是(2)中所举出的群.

(α,ii) 假如 $ba=a^2b$，我们将推导出 $b^{-1}a^2b=a$，从而

$$(b^{-1}a^2b)^2=b^{-1}a^4b=b^{-1}1b=1=a^2,$$

然而这是不可能的，因此我们必须断定

(α,iii) $ba=a^3b$，或者，等价地，$(ab)^2=1$. 由下面关系式

$$a^4=b^2=(ab)^2=1 \tag{2.50}$$

所定义的群事实上确实存在，它用 D_4 表示，称为 8 阶的**二面体群**(后面表(xi)). 它属于以后会讨论到的一类群，那时结合律将被证实(还参看习题 7).

(β) 假设 $b^2=a^2$. 在这种情况下 a 与 b 都是 4 阶的. ba 又一定是(2.48)最后三个元素之一，我们将依次考虑：

(β,i) 假如 $ba=ab$，这群是阿贝尔群. 元素 $c=ab^{-1}$ 是 2 阶的. 既然 $ba^{-1}=c^{-1}$ 是 2 阶的且 $b=c^{-1}a$，生成元 b 可以用 c 代替，因此八个元素可以写成象(2.48)中的那样，不过用 c 代替 b. 我们又得到群(2).

(β,ii) 关系式 $ba=a^2b$ 是不可能的，因为它会导致 $ba=b^2b$，即 $a=b^2$，这是不允许的.

(β,iii) 唯一剩下的选择，即 $ba=a^3b$，是可以实现的，我们将看到，这导致下列关系式所定义的群

$$a^4=1, \quad a^2=b^2, \quad ba=a^3b. \tag{2.51}$$

为了说明这样的群的确存在，我们构造一个忠实的矩阵表示，设

$$A=\begin{bmatrix}\sqrt{-1} & 0\\ 0 & -\sqrt{-1}\end{bmatrix},\quad B=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}.$$

读者不难证实这些矩阵在适当改变记号之后满足关系式(2.51)，也不难证实下面八个矩阵

$$I,A,A^2,A^3,B,AB,A^2B,A^3B$$

是不相同的，因此构成一个乘法矩阵群，它与按照(β, iii)所规定的群同构.

这群称为**四元数群**（后面表(xii)）. 我们想起四元数就是超复数

$$a_0 1+a_1 i+a_2 j+a_3 k,$$

此处系数 a_0,a_1,a_2,a_3 是实数，而符号

$$1,i,j,k$$

满足方程

$$i^2=j^2=-1,\quad ij=-ji=k,$$

或者，等价地，

$$i^{-4}=1,\quad i^2=j^2,\quad ji=i^3j.$$

除开记号不同，这与(2.51)一致.

总结以上对 8 阶群的讨论，我们附上五个可能的 8 阶抽象群的完整的乘法表

$$C_8=\mathrm{gp}\{a\},\quad a^8=1$$

	1	a	a^2	a^3	a^4	a^5	a^6	a^7
1	1	a	a^2	a^3	a^4	a^5	a^6	a^7
a	a	a^2	a^3	a^4	a^5	a^6	a^7	1
a^2	a^2	a^3	a^4	a^5	a^6	a^7	1	a
a^3	a^3	a^4	a^5	a^6	a^7	1	a	a^2
a^4	a^4	a^5	a^6	a^7	1	a	a^2	a^3
a^5	a^5	a^6	a^7	1	a	a^2	a^3	a^4
a^6	a^6	a^7	1	a	a^2	a^3	a^4	a^5
a^7	a^7	1	a	a^2	a^3	a^4	a^5	a^6

[表(viii)]

$$C_4 \times C_2 = \mathrm{gp}\{a\} \times \mathrm{gp}\{b\},\quad a^4 = b^2 = 1$$

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	ab	a^2b	a^3b	1	a	a^2	a^3
ab	ab	a^2b	a^3b	b	a	a^2	a^3	1
a^2b	a^2b	a^3b	b	ab	a^2	a^3	1	a
a^3b	a^3b	b	ab	a^2b	a^3	1	a	a^2

[表(ix)]

$$C_2 \times C_2 \times C_2 = \mathrm{gp}\{a\} \times \mathrm{gp}\{b\} \times \mathrm{gp}\{c\},\ a^2 = b^2 = c^2 = 1$$

	1	a	b	c	ab	ac	bc	abc
1	1	a	b	c	ab	ac	bc	abc
a	a	1	ab	ac	b	c	abc	bc
b	b	ab	1	bc	a	abc	c	ac
c	c	ac	bc	1	abc	a	b	ab
ab	ab	b	a	abc	1	bc	ac	c
ac	ac	c	abc	a	bc	1	ab	b
bc	bc	abc	c	b	ac	ab	1	a
abc	abc	bc	ac	ab	c	b	a	1

[表(x)]

二面体群：$a^4 = b^2 = (ab)^2 = 1$

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	1

[表(xi)]

四元数群：$a^4=1, a^2=b^2, ba=a^3b$

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	1	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	1
a^2b	a^2b	ab	b	a^3b	1	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	1	a^3	a^2

[表(xii)]

§ 15 乘积定理. 在本章开头我们定义了两个子集的乘积. 现在我们来考察两个集都是一个群的子群的情况. 我们将会看到两个子群的积不总是一个子群. 但是在有限子群的情况中可以得到关于乘积中元素个数的明确知识.

定理 5(乘积定理) (i) *设 A 与 B 是子群. 那么子集 AB 是一个群当且仅当*

$$AB=BA. \tag{2.52}$$

(ii) *在有限子群的情况中，设 $|A|=a, |B|=b, |A\cap B|=d$. 那么不论(2.52)是否成立，总有*

$$|AB|=|BA|=ab/d.$$

证明 (i) 因为 A 与 B 是子群，我们有 $A^2=A$ 及 $B^2=B$. 首

先，假设(2.52)成立，设 $H=AB$，那么

$$H^2=ABAB=A^2B^2=AB=H.$$

这证明了 H 的封闭性. 显然，$1\in H$，因为 $1\in A$ 及 $1\in B$. 最后假如 a 与 b 分别是 A 与 B 的任意元素，那么 $b^{-1}a^{-1}\in BA$，因而，由(2.52)，$b^{-1}a^{-1}\in AB=H$，即 $(ab)^{-1}\in H$，这就完成了 H 是群的证明.

反之，假设 $H=AB$ 是群，因而假如 a 与 b 分别是 A 与 B 的任意元素，那么 $ab\in H$，$a^{-1}b^{-1}\in H$，还有 $(a^{-1}b^{-1})^{-1}\in H$，即 $ba\in H$，这意味

$$BA\subset AB.$$

特别，$b^{-1}a^{-1}=a_1b_1$，此处 a_1 及 b_1 分别是 A 与 B 的某个元素，因而 $(b^{-1}a^{-1})^{-1}=ab=b_1{}^{-1}a_1{}^{-1}$，即

$$AB\subset BA.$$

因而我们断定 $AB=BA$.

(ii) 设 $D=A\cap B$. 因为 D 是 B 的子群，我们可以将 B 分解成对于 D 的陪集，比如说

$$B=Dt_1\cup Dt_2\cup\cdots\cup Dt_n, \tag{2.53}$$

此处

$$Dt_i\neq Dt_j，假如\ i\neq j \tag{2.54}$$

及

$$n=b/d. \tag{2.55}$$

用 A 左乘(2.53)，注意因为 $D\subset A$，故 $AD=A$. 我们得到

$$AB=At_1\cup At_2\cup\cdots\cup At_n. \tag{2.56}$$

我们断定(2.56)右边任意两个陪集没有一个公共元素；因为假如不是这样，我们将有下面这样形式的等式

$$u_1t_i=u_2t_j,$$

此处 $u_1,u_2\in A$ 及 $i\neq j$. 因此

$$t_it_j{}^{-1}=u_1{}^{-1}u_2.$$

于是根据(2.53)，上式左边的元素属于 B，而右边的元素属于 A. 因而每边都表示 D 的一个元素. 但是 $t_i t_j^{-1} \in D$ 意味 $Dt_i = Dt_j$，这与(2.54)矛盾. 因此(2.56)中的陪集是不相交的. 又因为每一陪集包含 a 个元素，我们有

$$|AB| = an = ab/d.$$

显然，以上的证明对 A 与 B 是对称的，所以也有 $|BA| = ab/d$.

§ 16. 双陪集. 我们曾经在 § 10 看到，一个群对于某一子群的陪集的分解，可以看作一个集相对于适当定义的等价关系划分成不同的等价类的例子.

现在，我们仿照福楼拜尼斯(Frobenius)的做法，讨论另一种等价关系，它涉及两个子群. 设 A 与 B 是 G 的子群，它们可以相同. 我们说两个元素 $x, y \in G$ 是等价的，写成 $x \sim y$，假如存在元素 $u \in A$ 和 $u \in B$ 使得

$$y = uxv. \tag{2.57}$$

容易验算这是 G 上的等价关系，因为

(i) $x \sim x$，因为我们可以取 $u=1, v=1$.

(ii) 假如 $x \sim y$，那么 $y \sim x$，因为(2.57)意味 $x = u^{-1}yv^{-1}$.

(iii) 假如 $x \sim y$, $y \sim z$，即 $y = uxv$, $z = u'yv'$，此处 $u' \in A$, $v' \in B$，那么 $z = (u'u)x(vv')$，所以 $x \sim z$.

因此，根据上面的等价关系的定义，集 G 可以分成不相交的等价类. 包含 x 的等价类是复形 AxB，它称为 G 对于 A 与 B 的双陪集. 我们从每一等价类中选择一个代表就得到分解式

$$G = \bigcup_{i \in I} At_iB, \tag{2.58}$$

此处 I 可能是无限的指标集，它与双陪集一一对应. 显然，(2.58)是左或右陪集分解式的推广，只要取 A 或 B 为平凡群{1}就可以看出这一点. 与单陪集分解式不同的是，(2.58)中的双陪集一般不具有相同的基数.

当 G 是有限群时，我们要进一步讨论这个问题. 设 $|G|=g$，$|A|=a$ 及 $|B|=b$. 首先，我们注意到复形 At_iB 与 $(t_i^{-1}At_i)B$ 具有相同基数，因为将 ut_iv 与 $t_i^{-1}(ut_iv)$ 对应是这两个集合的元素之间的一一对应，因此

$$|At_iB|=|(t_i^{-1}At_i)B|.$$

因为 $t_i^{-1}At_i$ 是一子群(参看 § 9)，及

$$|t_i^{-1}At_i|=|A|=a.$$

应用定理 5 到子群 $t_i^{-1}At_i$ 和 B，我们得出

$$|At_iB|=ab/d_i,$$

此处 $d_i=|t_i^{-1}At_i\cap B|$. 整理这些结果， 我们得到下面的定理.

定理 6 (Frobenius) 设 G 是 g 阶有限群，A 与 B 分别是 a 阶与 b 阶的子群. 那么存在元素 $t_1,t_2,\cdots,t_r$ 使得 G 是双陪集的不相交的并，即

$$G=At_1B\cup At_2B\cup\cdots\cup At_rB.$$

At_iB 中元素的个数是

$$ab/d_i,$$

此处

$$d_i=|t_i^{-1}At_i\cap B|.$$

从而

$$g=ab\sum_{i=1}^{r}d_i^{-1}. \qquad (2.59)$$

习 题

(1) 设 $D=X\cap Y$ 及 $M=\mathrm{gp}(X,Y)$，此处 X 与 Y 是群 G 的非空子集. 证明：假如 Z 是 G 的另一子集，则

$$X\cap Y\cap Z=D\cap Z, \mathrm{gp}\{X,Y,Z\}=\mathrm{gp}\{M,Z\}.$$

(2) 设 $D=A\cap B$，此处 A 与 B 是 G 的子群，证明：假如 $u,v\in At\cap Bs$，此处 $s,t\in G$，那么 $Du=Dv$. 导出当 $[G:A]$ 与 $[G:B]$ 是有限时，$[G:D]$ 也

$[G:A][G:B]$.（庞加莱定理）

(3) 证明：假如A与B是阶互素的有限子群，那么 $A\cap B$ 只包含单位元素.

(4) 证明一个阶为合数的有限群具有一个真子群.

(5) 找出 8 阶二面体群(表(xi))的所有 4 阶子群.

(6) 证明表 v(§ 4)的群可以用下面的关系式定义

$$c^2=d^2=(cd)^3=1.$$

(7) 设 $\varepsilon=\exp(2\pi i/n)$,此处 n 是比 1 大的正整数，证明矩阵

$$A=\begin{bmatrix}\varepsilon & 0\\ 0 & 1/\varepsilon\end{bmatrix}, B=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

形成 2 n 阶二面体群 $D_n=\mathrm{gp}\{a,b\}$ 的一个忠实表示. D_n 由下面的定义关系给出

$$a^n=b^2=(ab)^2=1.$$

(8) 设 $\theta=\exp(\pi i/m)$,此处 m 是大于 1 的正整数. 证明矩阵

$$A=\begin{bmatrix}\theta & 0\\ 0 & 1/\theta\end{bmatrix}, \quad B=\begin{bmatrix}0 & 1\\ -1 & 1\end{bmatrix}$$

形成 4 m 阶**双循环群**的一个忠实表示. 这群由下列关系式给出

$$a^{2m}=1,\ b^2=(ab)^2=a^m.$$

(9) 证明假如 12 阶的非交换群包含一个 6 阶元素，那么它或者与同阶的二面体群同构,或者与同阶的双循环群同构.

(10) 证明与 21 互素的剩余形成一个(乘法的)阿贝尔群,它与$C_6\times C_2$同构.

(11) 设 $X=\mathrm{gp}\{x\}$是由 x 生成的无限循环群，又设 $R=\mathrm{gp}\{x^r\}$，此处 r 是正整数. 证明$[X:R]=r$.

第三章　正规子群

§ 17. 共轭类. 在上一章中我们曾经讨论过将群G对于G的某一子群分成等价类的方法．现在我们将引入另一种等价关系．

定义 4　元素a与b称为在G中**共轭**，假如G中存在一个元素t使得

$$b=t^{-1}at. \tag{3.1}$$

我们说t将a变换成b．在现阶段，我们对完成变换的元素不特别感兴趣．应该注意，对于给定的a与b，可能不止一个元素t满足关系(3.1)．(3.1)式的右边有时缩写为a^t，即我们使

$$a^t=t^{-1}at. \tag{3.2}$$

假如对于某一t存在关系(3.1)，我们暂时写为$b\sim a$．我们来验证这是一个等价关系．因为

(i) $a\sim a$(自反性)，取$t=1$；

(ii) $b\sim a$蕴含$a\sim b$(对称性)．因为假如(3.1)适用，那么$a=tbt^{-1}=(t^{-1})^{-1}b(t^{-1})$，所以$a\sim b$．

(iii) 假如$a\sim b$及$b\sim c$，那么$a\sim c$(可递性)．因为我们已有$a=t^{-1}bt$及$b=s^{-1}cs$，消去b后，$a=(st)^{-1}c(st)$，即$a\sim c$．

而且，我们注意到共轭服从重要的乘法法则

$$(xy)^t=x^ty^t, \tag{3.3}$$

此处x,y,t是G的任意元素，因为

$$(xy)^t=t^{-1}xyt=(t^{-1}xt)(t^{-1}yt)=x^ty^t.$$

显然，(3.3)式可以推广到任意多个因子，因而

$$(x_1x_2\cdots x_n)^t=x_1^tx_2^t\cdots x_n^t.$$

在(3.3)中令$y=x^{-1}$，注意$1^t=1$，我们推导出

$$1=x^t(x^{-1})^t,$$

即

$$(x^t)^{-1}=(x^{-1})^t. \qquad (3.3)'$$

我们记得，在一个集上定义一个等价关系后，这个集就划分成为不相交的类，每类由与某一特殊元素等价的那些元素组成. 在目前情况中，这些类称为**共轭类**. 包括特殊元素 a 的共轭类以 (a) 表之，它包含 G 中所有与 a 共轭的元素，且包含 a 本身，因而

$$(a)=t_1^{-1}at_1\cup t_2^{-1}at_2^{-1}\cup\cdots.$$

我们可以假设 $t_1=1$. 假如 b 是不包含在 (a) 内的元素，那么 b 生成一个新的共轭类

$$(b)=s_1^{-1}bs_1\cup s_2^{-1}bs_2\cup\cdots.$$

共轭关系的可递性保证 (a) 与 (b) 没有公共元素. 用这种方法进行下去，我们得出 G 的共轭类分解式，因而

$$G=(a)\cup(b)\cup(c)\cup\cdots,$$

我们称 $a,b,c,\cdots$ 为不同类的代表，但是要记住这些代表不是唯一的；事实上，$(a)=(a')$ 当且仅当 $a'=x^{-1}ax(x\in G)$.

当 G 是无限时，可以存在无限多的共轭类，某一特殊的共轭类可能包含无限多元素. 重要的是，得到关于构成某一给定类的元素的更精确的知识，并且当类是有限时决定它的大小. 显然，类 (1) 只包含单独一个元素 1，因为对于所有属于 G 的 t，有 $t^{-1}1\,t=1$.

为了更详细地考查这个问题，我们引入**中心化子**这个概念. 设 a 是 G 的固定元素，用 $C(a)$ 表示 G 中所有与 a 交换的元素的集，因而

$$C(a)=\{t\in G\,|\,ta=at\}.$$

容易验证 $C(a)$ 是 G 的子群. 因为 (i) 假如 $s,\ t\in C(a)$，那么 $a(st)=sat=(st)a$，所以 $st\in C(a)$；(ii) $1\in C(a)$，及 (iii) 假如 $t\in C(a)$，那么 $t^{-1}a=at^{-1}$，即 $t^{-1}\in C(a)$.

附带提一下，除非 $G=\{1\}$，否则总有 $|C(a)|\geqslant 2$. 因为假如

$a=1$，那么$C(a)=G$；假如$a\neq1$，那么$a\in C(a)$及$1\in C(a)$.

其次，考虑G对于$C(a)$的陪集分解式，即

$$G=\bigcup_i C(a)t_i(i\in I),$$

此处I是对应的指标集.

我们断定$C(a)$的陪集与(a)中的元素一一对应，这个对应由下面的映射建立：

$$\theta: C(a)x\to x^{-1}ax. \quad (3.4)$$

首先我们必须证明θ具有明确的定义，记住$C(a)x$可以等同地写为$C(a)ux$，此处u是$C(a)$的任一元素. 因而我们必须证明用ux代x并不改变(3.4)的右边. 事实上，

$$(ux)^{-1}a(ux)=x^{-1}u^{-1}aux=x^{-1}ax,$$

因为$u\in C(a)$. 既然x是G的任一元素，映射θ显然是到类(a)上的满射. 最后，我们看出θ是单射，因为假如$x^{-1}ax=y^{-1}ay$，那么$xy^{-1}\in C(a)$，从而$C(a)x=C(a)y$. 因而，象所断定的那样，θ是双射.

我们整理这些结果如下：

命题 7 设a是G的元素，$C(a)$是a的中心化子. 那么共轭类的元素与G中$C(a)$的陪集一一对应，特别，当$C(a)$的指数是有限时，$|(a)|=[G:C(a)]$.

推论 假如G是g阶有限群，又假如h_a是(a)中元素的个数，那么$h_a|g$.

证明 设$|C(a)|=c_a$，那么由命题7，$h_a=g/c_a$，即$g=c_ah_a$.

假如有限群G具有k个不同的共轭类. 设$a_1(=1), a_2, \cdots, a_k$是一组代表，又令$h_i=|(a_i)|$，那么

$$G=(a_1)\cup(a_2)\cup\cdots\cup(a_k).$$

从而，计算这方程式每边元素的个数，

$$g=h_1+h_2+\cdots+h_k, \quad (3.5)$$

这个关系式称为群的**类方程**.

§ 18. 中心. 与G的每个元素交换的元素所形成的集Z称为G的**中心**. 因而

$$Z=\{z \mid tz=zt, 对所有的\ t\in G\}.$$

这是G的子群. 因为(i)假如$tz_1=z_1t$, 及$tz_2=z_2t$, 那么$tz_1z_2=z_1tz_2=z_1z_2t$, 所以$z_1z_2\in Z$;(ii)假如$tz=zt$,那么$z^{-1}t=tz^{-1}$,所以$z^{-1}\in Z$;(iii)$1\in Z$. 当然Z总是阿贝尔群,但是它可以是单位元群. 例如,在6阶非阿贝尔群中(参看§4表(v)), 中心就只包含单位元素,显然,$G=Z$当且仅当G是阿贝尔群.

中心的元素的特点是它本身形成一个共轭类, 因为假如z只与本身共轭,那么$t^{-1}zt=z$对所有的$t\in G$,这意味$z\in Z$.由于这个理由,中心元素有时称为**自共轭元素**. 下面的结果是有趣的,因为它证明一类重要的群存在非平凡中心.

定理 7 假如G是有限群,使得$|G|=p^m$,此处p是素数及$m>0$,那么G的中心具有p^μ阶,此处$0<\mu\leqslant m$.

证明 在目前情况下,类方程(3.5)成为

$$p^m=h_1+h_2+\cdots+h_k, \tag{3.6}$$

此处$h_\alpha \mid p^m(\alpha=1,2\cdots,k)$. 既然$p$是素数,这意味每一$h_\alpha$或者等于1或者等于$p$的幂. 我们已知$h_1=1$, 假设恰好存在$l(\geqslant 1)$个$\alpha$的值使得$h_\alpha=1$, 则我们能将(3.6)写成下面的形式

$$p^m=l+ps,$$

其中s是某一整数. 于是l可被p整除,因为l是正的,我们断定$l\geqslant p$. 因而至少存在p个自共轭元素,即Z是非平凡的. 既然Z是G的子群,拉格朗日定理提供了更进一步的知识,即$|Z|=p^\mu$,此处$0<\mu\leqslant m$.

§ 19. 正规子群. 中心化子的概念可以推广到G的任一非空子集,因而A的中心化子$C(A)$由G的所有那些元素组成,它们与A的每一元素交换,即

$$C(A)=\{t \mid ta=at\ 对于所有\ a\in A\}.$$

象先前那样，中心化子 $C(A)$ 总是 G 的子群，可能是单位元子群. 事实上 $C(A)$ 是群 $C(a)$ 的交集，此处 a 遍历 A. 当需要表示 $C(A)$ 与包含 A 的群 G 有关时，我们更精确地写成 $C_G(A)$. 注意，一般地说

$$C_G(G) = G \text{ 的中心}.$$

我们现在讨论一个不同的交换性概念，给出一非空子集 A，我们考虑 G 的这样一些元素 s，它们满足子集间的关系

$$sA = As. \tag{3.7}$$

因而(3.7)意味对于每一 $a \in A$，存在 $a_1, a_2 \in A$ 使得 $sa = a_1 s$ 及 $as = sa_2$. 我们留给读者直接去验证：那些满足(3.7)的元素 s 形成 G 的子群. 这子群称为 A 的**正规化子**，表示为 $N(A)$，或者更精确地表示为 $N_G(A)$. 显然，$C(A)$ 的每一元素肯定满足 (3.7)，因为它与 A 的每一元素交换. 因而

$$C(A) \leqslant N(A).$$

但是一般情况下正规化子大于中心化子.

我们特别对 A 是 G 的子群，比如说 H 的情况感兴趣. 象我们已经看见过的那样 (§ 9)，当 x 是 G 的任一元素，那么 $H' = x^{-1}Hx$ 也是子群，它与 H 同构，虽然一般情况下与 H 不相同，我们称 H 与 H' **共轭**. 可是通过不同的元素 x 与 y 的共轭可以产生同一子群. 事实上，方程

$$x^{-1}Hx = y^{-1}Hy \tag{3.8}$$

等价于 $Hxy^{-1} = xy^{-1}H$，所以 $xy^{-1} \in N(H)$. 因而(3.8)成立当且仅当 $x = sy$，此处 $s \in N(H)$. 群 H 本身也算作 H 的一个共轭，于是我们有 $H = s^{-1}Hs$ 当且仅当 $s \in N(H)$.

显然 $H \leqslant N(H)$，因为假如 $u \in H$，那么 $u^{-1}Hu = H$(参看 § 9，命题 3).

G 的最有趣的子群是它们的正规化子是整个 G 的那些子群. 当 $N(H) = G$ 时，我们说 H 是 G 的**正规子群**或**不变子群**而用专门

的符号表示：

$$H \lhd G.$$

让我们再详细讨论一下这个极端重要的概念．一个正规子群的特点是它除本身之外没有别的共轭子群，即

$$xH=Hx \text{ 或 } H=x^{-1}Hx，\text{对所有的 } x\in G. \tag{3.9}$$

更明确地说，假如 x 是 G 的任一元素及 u 是正规子群 H 的某一元素，那么存在一个元素 $u'\in H$ 使得

$$x^{-1}ux=u'.$$

实际上，为了证明 $H\lhd G$，只要验证对于所有 $x\in G$，

$$x^{-1}Hx\subset H \tag{3.10}$$

就可以了．因为假设情况是这样，我们就能以 x^{-1} 代 x，于是得到 $xHx^{-1}\subset H$，这等价于

$$H\subset x^{-1}Hx,$$

它与(3.10)一道意味 $H=x^{-1}Hx$．在每一个群 G 中，单位元子群 $\{1\}$ 及 G 本身是 G 的正规子群．一个大于 1 阶的群假如除这两个平凡正规子群外没有别的正规子群，则称为**单群**．当然，素数阶的群一定是单群，但是存在合数阶的单群的有趣例子(参看 **§41**)．阿贝尔群的每一子群自然是正规子群，因为(3.9)是交换性的推论．

为了验证 H 在 G 中是否是正规的，下面的方法经常用到：

(1) 假设 G 用生成元来表示(参看 **§12**)，比如说

$$G=\mathrm{gp}\{a,b,c,\cdots\}.$$

假如我们能证明

$$a^{-1}Ha=H, b^{-1}Hb=H, c^{-1}Hc=H, \cdots$$

那么 $a,b,c,\cdots$ 属于 $N(H)$．但是既然这些元素生成整个 G，我们推出 $G=N(H)$，即 $H\lhd G$．

(2) 假如所给的 H 用生成元来表示，比如说

$$H=\mathrm{gp}\{x_1,x_2,x_3,\cdots\}.$$

那么如果对每一 $t\in G$,

$$x_i^t\in H(i=1,2,3,\cdots),$$

则 $H\lhd G$. 因为由(3.3),这保证这些 x 的每一个(有限)乘积在 t 的共轭下仍旧属于H,所以 $t^{-1}Ht\subset H$.

例如,设G是 § 14 中表(xi)所表示的 8 阶二面体群,设

$$H=\text{gp}\{a\}$$

是 a 所生成的 4 阶循环群.显然,$a\in N(H)$. 另有 $bab^{-1}=a^3$, 因而 $bHb^{-1}\leqslant H$. 但H 和bHb^{-1}同构,因而有相同的阶,于是,$bHb^{-1}=H$.这意味 $b(=b^{-1})$属于 $N(H)$,由此证明了 $N(H)=G$.

我们接着将集中几个关于正规子群的基本事实.

(i) 中心总是正规子群. 因为条件(3.9),即 $x^{-1}Zx=Z$ 对所有 $x\in G$ 肯定满足. 事实上,甚至对于Z的任一元素 z, 我们都有 $x^{-1}zx=z$.

(ii) 假如 $N_1,N_2,\cdots,N_r$是正规子群,则它们的交集也是正规子群.因为既然 $x^{-1}N_ix=N_i(i=1,2,\cdots,r)$,我们导出

$$x^{-1}(N_1\cap N_2\cap\cdots\cap N_r)x=N_1\cap N_2\cap\cdots\cap N_r.$$

(iii) 子群H在G中是正规的,当且仅当它是G的共轭类的并集,即

$$H=(1)\cup(u)\cup(v)\cup\cdots. \qquad (3.11)$$

因为(3.11)显然等于说,只要w属于 H, 那么 $x^{-1}wx$ 也属于 H, 此处x是G的任一元素. 这意味 $x^{-1}Hx\subset H$,因而 $H\lhd G$.

(iv) 假如H在G中的指数是 2,那么$H\lhd G$. 在这情况下恰好存在两个G中的H陪集,一个是H,另一个是 $G\backslash H$, 即那些不属于H的G的元素. 因而,假如 $t\in G\backslash H$,那么 $G\backslash H=Ht$. 同样的讨论可用于左陪集,所以 $G\backslash H=tH$,从而 $Ht=tH$,只要 $t\notin H$. 另一方面,假如 $w\in H$,那么 $H=Hw=wH$. 因而方程 $xH=Hx$ 对所有 $x\in G$ 成立,即 $H\lhd G$. 例如,利用这个方法可以立刻证明 gp$\{a\}$是二面体群的正规子群.

§ 20. 商群. 正规子群的重要性主要在于这个事实：正规子群的陪集的集合能够具有群的结构. 假设 $H\lhd G$，并考虑两个陪集 Hx 与 Hy 的积. 因为 $xH=Hx$ 及 $H^2=H$，我们得出

$$HxHy=HHxy=Hxy, \tag{3.12}$$

因而两个陪集的积还是一陪集. 注意到(3.12)确实是陪集间的关系，即它与陪集的代表无关是极其重要的. 更准确地说，我们断定，假如 $Hx=Hx'$ 及 $Hy=Hy'$，那么 $Hxy=Hx'y'$. 事实上，我们的假设蕴含 $x'=ux$, $y'=vy$，此处 $u, v\in H$. 那么 $x'y'=uxvy=uv'xy$，此处 v' 是 H 的某一适当的元素. 因而象所要求的那样，我们有 $Hx'y'=Hxy$.

假如我们利用对于 H 的等价性概念，事情可以稍微不同的方式提出. 象在 **§ 10** 上所说的那样，假如存在元素 $u\in H$ 使得 $x'=ux$，我们写成 $x\sim x'$. 因为 $Hx=xH$，我们也可以换一种规定 $x'=xu'$，此处 $u'\in H$. 因此某一特殊元素 $x\in G$ 的等价类 $[x]$ 是与陪集 $Hx(=xH)$ 等同的. 于是(3.12)表示了等价类的乘法，即

$$[x][y]=[xy]. \tag{3.13}$$

它与类的代表无关.

由于(3.12)，在子集的乘法下陪集集合是封闭的. 这产生了一个希望，即陪集的集合实际上形成一个群. 验证结合律是不存在困难的，因为它适用于所有的子集(见 **§ 8**). 对于陪集的乘法，单位元素是作为陪集的群 H，因为

$$H(Ht)=(Ht)H=Ht.$$

最后，Ht 的逆元素是陪集 Ht^{-1}，因为 $(Ht)(Ht^{-1})=H=(Ht^{-1})(Ht)$. 我们所构造的群用 G/H 表示，称为 G 关于 H 的**商群**. G/H 的阶等 H 在 G 中的指数，即

$$|G/H|=[G:H]. \tag{3.14}$$

商群的概念不但对于群论是基本的，而且实际上是数学中最重要的概念之一. 因此我们重复某些与商群有关的要点.

(1) G/H 的元素是H的不同陪集，合成规则是子集的乘法（或者是陪集的加法，当G用加法写出时（参看 § 10 末尾））．

(2) 单位（零）元素是群 H，它当作一个陪集．

(3) 我们究竟用右或左陪集是没有关系的，因为H是正规的，因而 $Ht=tH$．

(4) 记住某一特殊陪集的代表不是唯一的（见 § 10）．

(5) 商群这一名词及 G/H 这一记号只有当H是正规子群时才用．

接着我们将要讨论几个例子来阐明商群的概念．

(i) 设 Z 是所有整数的（加法）群，又设 $m>1$ 是一个固定的整数，那么集

$$H: 0, \pm m, \pm 2m, \cdots, \pm km, \cdots$$

形成 Z 的子群．因为 Z 是阿贝尔群，所以H是正规子群．假如 x 是任一整数，我们能写成 $x=qm+r$，此处 $0\leqslant r<m$．因为 qm 在 H 中，x 位于陪集 $H+r$ 中（见 § 10 末尾）．考虑到 r 的可能值，我们看到，

$$H(=H+0), H+1, H+2, \cdots, H+(m-1) \qquad (3.15)$$

是不同的陪集，即 Z/H 的元素．这些陪集与 Z_m的元素一一对应（见 § 3(1.17)）．假如，Z_m的元素暂时用 $\bar{0}$，$\bar{1}$，$\cdots$，$\overline{m-1}$表示，我们可以将这对应表示如下：

$$H+r\longleftrightarrow\bar{r}.$$

我们注意到在这个对应下合成规则被保持．因为

$$(H+r)+(H+s)=H+t,$$

此处 $t\equiv r+s \pmod m$ 及 $0\leqslant t<m$，根据 Z_m中的合成规则，这恰为

$$\bar{r}+\bar{s}=\bar{t},$$

因此我们断定

$$Z/H\cong Z_m.$$

(ii) 在四元数群中(§ **14**，表(xii))，元素 $a^2=b^2$ 显然与 a 及 b 交换．因为 a 与 b 生成整个群，因而 $a^2=b^2$ 与四元数群的每一元素交换．因此

$$H=1\cup a^2 \quad (a^4=1)$$

是一正规子群(实际 H 是中心)．G/H 的元素可以列举如下

$$H, Ha, Hb, Hab. \tag{3.16}$$

因为我们预先知道存在 $[G:H]=8/2=4$ 个陪集，而(3.16)中的陪集是不同的，这一点易于验证，例如 $Hb=b\cup a^2b$．因为 G/H 是 4 阶的群，因此一定或者与 C_4 或者与 $C_2\times C_2$ 同构(见 § **14**)．注意到 G/H 的每一元素的平方等于单位元素 H，这个问题就完全解决了．事实上因为 $a^2\in H$，故 $(Ha)^2=Ha^2=H$，类似地 $(Hb)^2=Hb^2\in H$；最后，既然 G/H 必然是 4 阶阿贝尔群，我们有

$$(Hab)^2=(Ha)^2(Hb)^2=H.$$

因而 $G/H\cong C_2\times C_2$(见 § **13**，命题 6，)

(iii) 设 $G=GL(n,F)$ 是 F 上 n 次一般线性群(见 § **3** 例(iv))，即所有非奇异 $n\times n$ 矩阵 $\boldsymbol{a}=(a_{ij})$ 的集，其中 $a_{ij}\in F$．那么行列式是 1 的矩阵形成一个子群 U．因为假如 $\det \boldsymbol{u}=\det \boldsymbol{v}=1$，那么 $\det(\boldsymbol{uv})=1$；还有 $\det \boldsymbol{u}^{-1}=1$ 以及单位矩阵属于 U．此外 $U\lhd G$，因为假如 $\boldsymbol{x}\in G$，那么 $\det(\boldsymbol{x}^{-1}\boldsymbol{ux})=\det \boldsymbol{u}=1$．现在容易看出两个矩阵 $\boldsymbol{a}$ 与 $\boldsymbol{b}$ 属于 U 的同一陪集当且仅当 $\det \boldsymbol{a}=\det \boldsymbol{b}$，因为这等价于 $\boldsymbol{ab}^{-1}\in U$，因而 $\det(\boldsymbol{ab}^{-1})=1$．显然行列式可以取 F 中任一非零值，F 的非零元素集常常以 F^* 表示，因而

$$G/U\cong F^*.$$

例如，G 中关于 U 的横截(见 § **10**)由对角线矩阵 $\mathrm{diag}(d,1,1,\cdots,1)$ 所提供，此处 d 遍历 F^*．

最后，我们指出一个关于中心的结论，它有时是有用的．

命题 8 假如 G 是非阿贝尔群，具有中心 Z，那么 G/Z 决不是循环的．

证明　假如G/Z是循环群，那么Z的所有陪集可以表示为Zt^i，此处t是G的不在Z中的适当元素，$i=0,\pm1,\pm2,\cdots$．现在假设x与y是G的任意元素，分别属于陪集Zt^k与Zt^l，我们将有

$$x=z_1t^k,\qquad y=z_2t^l,$$

此处$z_1,z_2\in Z$．因而

$$xy=z_1t^kz_2t^l=z_1z_2t^{k+l}=yx.$$

即G是阿贝尔群，与我们的假设矛盾．

推论　阶是p^2(p是素数)的群必然是阿贝尔群．

证明　由定理7，$|Z|$等于p或p^2．假如$|Z|=p^2$，那么$G=Z$，因而这群是阿贝尔群．假如$|Z|\neq p^2$，那么$|Z|=p$及$|G/Z|=p$．因而G/Z将是循环群．而由上一命题，这种情形是排除在外的．

§ 21．同态． 群的结构中包含给出所有可能的乘积ab的法则．在第一章(§ **4**)我们讨论了两个群是同构的情况，即它们具有相同的结构．现在我们就要考虑一种更一般的关系，在这种关系下，群有着相似的"结构"，或者用希腊语来说，我们将要讨论**同态群**．为了把这概念讲得更精确，我们假设有一个群G到群G'内的映射

$$\theta:G\to G'.$$

象以前一样，$x\in G$的象用$x\theta$表示，所以$x'=x\theta$是G'中由映射θ与x相联系的唯一元素．假如，对于所有$x,y\in G$，

$$(x\theta)(y\theta)=(xy)\theta,\qquad(3.17)$$

我们称θ是同态映射，或者更简短地说，θ是G到G'内的同态．(3.17)是我们加在θ上的唯一条件．下面几点必须特别注意：

(i) 设1与$1'$分别是G与G'的单位元素．取$x=y=1$，我们有$(1\theta)^2=1\theta$．因而1θ是G'的幂等元素，因而(见§ **2**)

$$1\theta=1'.\qquad(3.18)$$

即每一同态映射将G的单位元素映射到G'的单位元素．而且，假如我们设$y=x^{-1}$，那么从(3.17)推导出

$$x^{-1}\theta=(x\theta)^{-1}. \tag{3.19}$$

(ii) 我们不要求映射是一对一的，因而可能发生 $x_1\theta=x_2\theta$，而 $x_1\neq x_2$. 可是假如等式 $x_1\theta=x_2\theta$ 总蕴含 $x_1=x_2$，那么我们说 θ **是单一同态或单的.**

(iii) 一般并不假定 θ 是满的，换句话说，可以存在 G' 的元素它们不是 G 的元素的象. 象的集用 $\mathrm{im}\,\theta$ 表示，或者更方便地，用 $G\theta$ 表示容易看出 $G\theta$ 是 G'的子群(它可以与 G' 重合). 事实上，假如$x',y'\in G\theta$，则存在元素 $x,y\in G$，使得 $x'=x\theta$，$y'=y\theta$，因而 $x'y'=(xy)\theta\in G\theta$. 由(3.18)，还有 $1'\in G\theta$ 及$(x')^{-1}\in G\theta$，假如$x'\in G\theta$. 另一方面，如果 θ 是满的，即假如

$$G\theta=G', \tag{3.20}$$

我们称 θ 为**满同态**. 同构的特点(按以前的意义)是它既是单的又是满的，或者更简短地说，它是**双的**. 在这种情况下我们继续用这记号 $G\cong G'$.

接着我们将要证实一件重要的事实，即 G 的每一同态映射与 G 的一个正规子群相联系. 设K是G的映射到 $1'$ 的元素的集，这个集称为 θ 的**核**，经常写为 $\ker\theta$. 首先，我们将要证明K是G的子群；假如$u,v\in K$，那么$u\theta=v\theta=1'$，因而，由(3.17)，$(uv)\theta=1'$；由(3.18)，有 $1\in K$；由 (3.19)，$u^{-1}\in K$. 此外，K 还是一个正规子群，因为假如 $x\in G$ 及 $u\in K$，那么

$$(x^{-1}ux)\theta=(x^{-1}\theta)(u\theta)(x\theta)=(x\theta)^{-1}1'(x\theta)=1',$$

这意味 $x^{-1}ux\in K$. 因而我们已经验证(3.10)对群 K适用，即

$$K\lhd G. \tag{3.21}$$

当然，可能发生K是 G的单位元子群. 在这一方面，注意下面的结果是有用的.

命题 9　同态 θ 是单的当且仅当 $\ker\theta$ 只包含单位元素.

证明　假设 θ 是单的，设 $u\in\ker\theta$，那么 $1\theta=u\theta=1'$. 因为 θ 是单的，因而 $u=1$. 反之，假定 $\ker\theta=\{1\}$，又假设 $x\theta=y\theta$，那么

$(xy^{-1})\theta=(x\theta)(y^{-1}\theta)=1'$. 因而 $xy^{-1}\in\ker\theta$,因此 $xy^{-1}=1$,即 $x=y$,这证明了 θ 是单的.

回到一般情况，我们现在要证实群论中最重要的事实之一.

定理 8(**第一*同构定理**)　*设 $\theta:G\to G'$ 是 G 到 G' 内的一个同态,具有象群 $G\theta$ 与核 K,那么*

$$G/K\cong G\theta. \tag{3.22}$$

证明　我们必须在 (3.22) 中的两个群之间构造一个双射同态. 这可以用映射 ϕ 来完成，它虽然一般与 θ 不同,但与 θ 有关，或者是从 θ 导出的. 我们记得,G/K 的元素是陪集 Kx,而 $G\theta$ 的元素是形为 $x\theta$ 的元素，此处 $x\in G$，而所有 Kx 的元素具有相同的象. 因此试探着建立一个一一对应 ϕ,它定义为

$$(Kx)\phi=x\theta. \tag{3.23}$$

虽然可以证明这个 ϕ 是所要求的,但是定义 (3.23) 没有进一步的证明是不能接受的.因为我们知道 Kx的生成元素 x不是唯一的).(§ 10,命题5),于是我们必须证明,只要

$$Kx=Ky, \tag{3.24}$$

那么 $x\theta=y\theta$. 只有在这情况下 ϕ 才是由 (3.23) 定义好的，才可防止不幸的不相容性. 因为(3.24)等于说 $y=ux$,此处 $u\in K$.由 K 的定义,$u\theta=1'$,因此 $y\theta=u\theta x\theta=x\theta$，正象所要求的那样. 现在我们能够着手证明 ϕ 具有我们所寻求的全部性质.

(1) ϕ 是同态:因为

$$(Kx)\phi(Ky)\phi=x\theta y\theta=(xy)\theta=(Kxy)\phi.$$

(2) ϕ 是满的：这是明显的,因为在(3.23)中 x 可以是 G 的任一元素,所以所有象元素 $x\theta$ 可以用 ϕ 得到.

(3) ϕ 是单的:我们需要证明

$$(Kx)\phi=(Ky)\phi \tag{3.25}$$

---

* 我们将看到，有好几个同构定理. 但是,关于它们的编号在文献中是不一致的.

蕴含 $Kx=Ky$. 假如(3.25)成立，那么由 ϕ 的定义 $x\theta=y\theta$. 这意味 $xy^{-1}\in K$,它等价于 $Kx=Ky$.

这就完成了定理的证明. 这个定理可以说成：G 的每一个同态象与 G 的某一个商群同构,即与关于核的商群同构.

为了使描述更为完整，我们指出 G 的任一正规子群作为一适当的同态的核而出现. 设 $N\lhd G$,考虑映射 $\nu:G\to G/N$ 定义为

$$x\nu=Nx(x\in G). \tag{3.26}$$

于是,在这情况下,$G'=G/N$. 容易验证(3.26)是一同态. 因为

$$(x\nu)(y\nu)=NxNy=Nxy=(xy)\nu.$$

显然,事实上 ν 是满同态,因为在(3.26)中,x 可以是 G 的任一元素,所以全部 G/N 都被包括了. ν 的核包含这样一些元素 $u\in G$,对于它们,$Nu=N$(G/N 中的单位元素),这等价于条件 $u\in N$. 因而 $\ker\nu=N$. 在(3.26)中所定义的映射称为 G 到 G/N 上的**自然映射**.

我们用§20中的例(iii)作为例证,此处 $G=GL(n,F)$. 假如 $\boldsymbol{a}\in G$,我们考虑同态

$$\delta:G\to F,$$

它定义为

$$\boldsymbol{a}\delta=\det\boldsymbol{a}.$$

在这情况中,$G\delta=F^*$,核由群 $U=\{\boldsymbol{a}\mid\det\boldsymbol{a}=1\}$组成. 它自然是 G 的正规子群. 由定理8,我们有

$$G/U\cong F^*,$$

与前面的结果一样.

第一同态定理使我们比较清楚地看出同态 $\theta:G\to G'$ 的效力: Kx 的所有元素具有象 $x'=x\theta$;特别,当$|K|$有限时,象群 $G\theta$ 恰好被覆盖$|K|$次. 此外,当指数$[G:K]$有限时,我们有

$$|G\theta|=[G:K]. \tag{3.27}$$

§22. 商群的子群. 设 $N\lhd G$ 是 G 的正规子群. 我们想要考查

G/N 的子群，研究它们与 G 的子群的关系．为了避免混淆，必须暂时对 G/N 的元素引入一个稍微精致一点的记号．G/N 的一个典型的元素将写为 (Nx)，以区别于由 $|N|$ 个 G 的元素组成的子集 Nx．G/N 的一个子群 A' 是某些元素的集合，比如说

$$A'=(N)\cup(Na)\cup(Nb)\cup\cdots, \tag{3.28}$$

关于 G/N 中的合成规则它们满足群的公理．去掉括号我们得到 G 的一个子集

$$A=N\cup Na\cup Nb\cup\cdots. \tag{3.29}$$

我们断定，事实上 A 是 G 的子群．显然 $N\subset A$，因而 $1\in A$．其次，假如 x 与 y 是 A 的元素，那么 (Nx) 与 (Ny) 是 A' 的元素，因为 A' 是一个群，$(Nxy)\in A'$，这意味 $xy\in A$．最后，假如 $x\in A$，那么 $(Nx^{-1})\in A'$，因而 $x^{-1}\in A$．因此我们已经证明 A 是一个群，更准确地说

$$N\leqslant A\leqslant G. \tag{3.30}$$

反之，假如 A 是 G 的任一满足 (3.30) 的子群，我们注意到，事实上，$N\lhd A$．因为关系式 $x^{-1}Nx=N$ 对所有 G 中的 x 适用，因而特别对于所有 A 中的 x 也适用．因此构造商群是合法的．现在假如(3.29)是 A 对于 N 的陪集分解，那么，加上括号，我们得到 A/N，它是 G/N 的子群．显然，G/N 的不同子群 A' 与 B' 导致 G 的不同子群 A 与 B，它们都包含 N．反过来也是正确的．因而在 G/N 的子群与 G 的那些包含 N 的子群之间存在一个一一对应．

了解 G/N 的正规子群关于这一点怎样描述是有趣的．我们可以假定这样的子群以 A/N 的形式表示，此处 A 满足(3.30)．于是

$$A/N\lhd G/N \tag{3.31}$$

当且仅当，对每一 $x\in G$ 及每一 $a\in A$，

$$(Nx)^{-1}(Na)(Nx)=(Nx^{-1}ax)\in A/N,$$

这等价于条件

$$x^{-1}ax\in A.$$

换句话说，$A\lhd G$. 我们总结这些结果如下：

命题 10 所有 G/N 的子群可以表成 A/N，此处

$$N\leqslant A\leqslant G,$$

以及 $A/N\lhd G/N$ 当且仅当

$$N\lhd A\lhd G.$$

转到 G/N 中来考虑，假定(3.31)满足，我们能够构造商群

$$(G/N)/(A/N).$$

幸好，由于下面一个定理，使形成商群的商群的复杂性不是很难对付.

定理 9(第二同构定理) 设 $N\lhd G$ 及 A 是 G 的正规子群，使得

$$N\lhd A\lhd G.$$

那么

$$(G/N)/(A/N)\cong G/A. \tag{3.32}$$

证明 考虑映射

$$\phi:G/N\to G/A,$$

它由以下规则定义

$$(Nx)\phi=(Ax)(x\in G). \tag{3.33}$$

首先，我们必须验证(3.33)的确是一个有意义的定义. 不变更陪集 Nx，(3.33)左边的元素 x 可以用 ux 代替，此处 $u\in N$，我们必须证明这代替不会变更(3.33)的右边. 因为 $N\leqslant A$，我们有 $u\in A$，所以 $Au=A$(§ 9，命题 3). 从而 $Aux=Ax$，正象所要求的那样. 其次我们看到 ϕ 是同态. 由于 A 的正规性，

$$(Nx)\phi(Ny)\phi=(Ax)(Ay)=(Axy)=(Nxy)\phi.$$

显然，ϕ 是满的，因为，在(3.33)中，x 是 G 的任意元素，所以 A 的所有陪集都会在(3.33)的右边出现，因而

$$(G/N)\phi = G/A. \tag{3.34}$$

剩下需寻求 $\ker\phi$. 现在 $(Nx)\in\ker\phi$ 当且仅当 $(Ax)=(A)$, A 是 G/A 的单位元素. 这等价于条件 $x\in A$. 因而 $\ker\phi$ 是陪集 (Na) 的并集,此处 a 遍历 A,换句话说

$$\ker\phi = A/N. \tag{3.35}$$

利用(3.34)及(3.35). 我们看出(3.32)是第一同态定理的直接推论▲

我们再一次回到同态的一般情况

$$\theta: G\to G'. \tag{3.36}$$

要问这个映射如何影响 G 的某一给定的子群 A. 这是指我们考虑限制映射

$$\theta_A: A\to G', \tag{3.37}$$

它由下面明显的规则所定义

$$a\theta_A = a\theta \quad (a\in A).$$

引进新符号 θ_A 似乎是多此一举,事实上 θ 与 θ_A 之间的区别有时确被忽略. 但是可以坚持(3.36)与(3.37)是不同的映射, 因为它们有着不同的"定义域". 象在所有同态映射中那样,象群

$$A' = A\theta_A (= A\theta)$$

是 G' 的子群,而 θ_A 的核显然由 A 中属于 θ 的核内的元素所组成,即

$$\ker\theta_A = A\cap\ker\theta. \tag{3.38}$$

值得更详细地考虑,当自然满同态

$$\nu: G\to G/N, \quad x\nu = (Nx)$$

限制到 G 的子群 A 中时,会产生什么结果. 这一象群可以明确地写成

$$A' = A\nu_A = \bigcup_a (Na), \tag{3.39}$$

此处 a 遍历 A,要注意这个并集可能包含多余的项. 另一方面, A' 是 G/N 的子群,正象我们在前面所看到的那样, 它一定具有形式

$A'=B/N$,此处 $N\leqslant B\leqslant G$. 在目前情况下,我们不能说 $B=A$,因为 A 不必包含 N,所以 A/N 可能没有意义. 寻求 B 的方法已在前面给出,这方法就是将(3.39)中的括号去掉,因而

$$B=\bigcup Na \quad (a\in A).$$

这可以更精确地用子集记号表示出来,即

$$B=NA.$$

用另一种方法验证 B 是一个子群是有益的. 因为既然 N 是正规的,$Na=aN$ 对每一个 $a\in A$ 成立,因此 $NA=AN$. 因而由乘积定理(§ 15),B 是一个群. 因而我们注意到

$$A\nu_A=NA/N. \tag{3.40}$$

其次,因为 $\ker\nu=N$,我们从(3.38)推出

$$\ker\nu_A=A\cap N. \tag{3.41}$$

我们注意到,作为一个核,$A\cap N$ 在 A 中是正规的.

将第一同构定理应用到 ν_A 上,有

$$A/\ker\nu A\cong A\nu_A$$

将(3.40)及(3.41)代入上式,我们将结果写在下面:

定理 10(第三同构定理) *设 N 是正规子群,A 是 G 的任一子群,那么*

$$\frac{A}{A\cap N}\cong\frac{NA}{N}.$$

值得考虑关于正规子群的内直积(§ 13). 假如

$$G=H\times K, \tag{3.42}$$

那么 K 的每一元素与 H 的每一元素交换,因而假如 $v\in K$,我们肯定有 $v^{-1}Hv=H$. 还有假如 $u\in H$,那么 $u^{-1}Hu=H$(§ 9,命题 3). 因为每一元素 $x\in G$ 可以表为 $x=uv$,那么 $x^{-1}Hx=H$. 因此 $H\lhd G$. 类似地可证 $K\lhd G$,即*在一直积中,每一因子是正规子群*.

其次,我们注意到

$$G/K \cong H. \tag{3.43}$$

假如我们令 $K=N$，$H=A$，注意到 $KH=H\times K=G$，$H\cap K=\{1\}$，那么(3.43)立即从第三同构定理得出. 或者，利用更直接的论证. 我们注意到 G 中 K 的陪集的形式是 Ku，此处 $u\in H$. 因为假如 $x=uv(u\in H, v\in K)$是 G 的任意元素，那么 $Kx=Kuv=Kvu=Ku$，因为 $Kv=K$. 还有，假如 $Ku_1=Ku_2$，此处 $u_1,u_2\in H$，那么 $u_1u_2^{-1}\in H\cap K=\{1\}$，因此 $u_1=u_2$. 因而

$$Ku\to u$$

提供了在群 G/K 与 H 之间的双射同态.

显然，由于对应

$$(u,v)\longleftrightarrow(v,u) \quad (u\in H, v\in K),$$

有

$$H\times K\cong K\times H.$$

§ 23. 导出群. 对于群 G 的任意两个元素 x 与 y，我们定义它们的换位子为

$$[x,y]=x^{-1}y^{-1}xy.$$

显然，$[x,y]=1$ 当且仅当 $xy=yx$. 我们对于当 x 与 y 遍历 G 时所有换位子的集感兴趣，这个集一般并不形成一个群，因为两个换位子的积不是总能够表成一个换位子(这是一件怪事，以致这种失败仅在相当复杂的群中才变得明显). 无论如何，我们可以构造一个群，它由所有的换位子所生成，这个群称为 G 的**导出群或换位子群**，而常用 G' 表示，即

$$G'=\mathrm{gp}\{[x,y]\mid x,y\in G\}. \tag{3.44}$$

因而 G' 的典型元素是有限个换位子的积. 显然，$G'=\{1\}$ 当且仅当 G 是阿贝尔群. G' 的主要性质搜集在下面的定理中.

定理 11 (i) 导出群 G' 是 G 的正规子群，而 G/G' 是阿贝尔群. (ii) 假如 H 是 G 的任一正规子群，使得 G/H 是阿贝尔群，那么 $G'\leqslant H$.

证明 (i) 为了证明$G'\lhd G$,只要证明

对所有 $t\in G$,

$$[x,y]^t\in G'$$

即可(见(3.2)与(3.10)). 由规律(3.3)与(3.3)′,我们有

$$[x,y]^t=[x^t,y^t].$$

既然右边是一个换位子,它就属于G'. 因而$G'\lhd G$. 其次,我们将证明陪集$G'x$与$G'y$交换,或者,用不同的符号,

$$[Gx',G'y]=G'.$$

因为$[x,y]\in G'$,所以

$$[G'x,G'y]=(G'x)^{-1}(G'y)^{-1}(G'x)(G'y)$$
$$=G'x^{-1}y^{-1}xy=G'[x,y]=G'.$$

因而G/G'是阿贝尔群.

(ii) 假如$H\lhd G$,我们只要用H代G'重复上面的计算,就能得出

$$[Hx,Hy]=H[x,y].$$

当G/H是阿贝尔群时,左边约化到G/H的单位元素,即H,于是我们推导出$[x,y]\in H$. 因为x与y是任意的,那么G'的每一生成元属于H,从而$G'\leqslant H$.

我们以证明下面的结果来结束本节.

命题 11 设A与B是G的正规子群,使得$A\cap B=\{1\}$. 那么A的每一元素与B的每一元素交换.

证明 考虑换位子

$$c=a^{-1}b^{-1}ab,$$

此处a与b分别是A与B的任意元素. 既然$A\lhd G$, 那么$a_1=b^{-1}ab\in A$,因此$c=a^{-1}a_1\in A$,类似地可证$c\in B$.因而$c\in A\cap B=\{1\}$,从而$c=1$,即$ab=ba$.

§ 24. 自同构. 当G的象群与G重合时,出现一个有趣的G的同构类型. G到本身上的同构

$$\alpha: G \to G$$

称为自同构. 特别 α 是 G 到自身上的双映射,即 α 置换 G 的元素. 当然,反过来就不一定正确,因为除此之外 α 还必须满足关系

$$(xy)\alpha=(x\alpha)(y\alpha)(x, y \in G). \tag{3.45}$$

应用 § 6 中的讨论，我们断定 G 的所有自同构的集合在映射的合成下形成一个群. 假如

$$\beta: G \to G$$

是另一个自同构，我们用 $\alpha\beta$ 代替 $\alpha \cdot \beta$ 表示 α 与 β 的积. 因而 $\alpha\beta$ 在元素 $x \in G$ 上的作用用下面的规律定义：

$$x(\alpha\beta)=(x\alpha)\beta.$$

G 的所有自同构的群以 $A(G)$ 表示,称为 G 的**自同构群**. $A(G)$ 的单位元素是恒等自同构 ι,它使 G 的每一元素不变,即

$$x\iota=x(x \in G). \tag{3.46}$$

α 的逆元素以 α^{-1} 表示，因而 $x\alpha^{-1}$ 是 G 的唯一元素 y 它满足 $y\alpha=x$;对每一 x，这样的元素存在,因为 α 是满的.

既然 α 是单的,所以 $\ker \alpha=\{1\}$. 这意味着 α 保持每一元素的阶. 因为假如 $y=x\alpha$ 及 $x^m=1$,那么由(3.45),

$$1=x^m\alpha=(x\alpha)^m=y^m,$$

因而 y 的阶不大于 x 的阶. 用 α^{-1} 代替 α，我们导出相反的不等式. 因而 x 与 y 具有相同的阶,它可以是无限大. 我们将 G 的固定元素 t 与映射 τ

$$\tau: G \to G$$

联系,τ 由下式给出

$$x\tau=x^t(=t^{-1}xt)(x \in G). \tag{3.47}$$

等式(3.3)说明 τ 是 G 到本身内的同态. 实际上它是一个自同构. 因为 $x^t=1$ 意味 $x=1$，因而 τ 的核缩减到单位元素. 从而，由命题 9,τ 是单的.还有,假如 y 是 G 的任一元素,则存在 x 使得 $x^t=y$,即 $x=tyt^{-1}$,因而 τ 是满的. 象(3.47)这样由共轭导出的自同

构称为G的**内自同构**. 不是内自同构的自同构称为**外自同构**.

下面，我们证明所有内自同构的集合$I(G)$在映射的合成下形成一个群. 比如，设σ是另一个由下式给出的内自同构

$$x\sigma=s^{-1}xs \quad (x\in G).$$

那么

$$x\tau\sigma=(t^{-1}xt)\sigma=s^{-1}t^{-1}xts$$
$$=(ts)^{-1}x(ts),$$

即

$$x^t x^s=x^{ts}. \tag{3.48}$$

因而合成映射$\tau\sigma$对应于通过ts产生的共轭. 这证明了$I(G)$的封闭性. 显然，$\iota\in I(G)$，因为我们可以取$t=1$，τ^{-1}对应于通过t^{-1}产生的共轭，即

$$x\tau^{-1}=txt^{-1} \quad (x\in G).$$

关于群$I(G)$更准确的结果由下面的命题所提供.

命题 12 设Z是G的中心，那么

$$I(G)\cong G/Z.$$

证明 元素t与由t所导出的内自同构τ之间的对应确定为映射

$$\Phi: G\to I(G), \tag{3.49}$$

Φ定义为

$$t\Phi=\tau \quad (t\in G).$$

于是等式(3.48)说明$(ts)\Phi=(t\Phi)(s\Phi)$，即Φ是同态. 显然，Φ是满的，因为每一个内自同构都由Φ作用在一适当的G的元素上而得到，因而

$$G\Phi=I(G).$$

其次，我们想要求$\ker\Phi$. 因为$t\in\ker\Phi$当且仅当由t导出的内自同构是恒等自同构

$$x^t=x \quad (x\in G).$$

但是这等式等于说 $t\in Z$. 因而 $\ker\Phi=Z$. 应用第一同构定理立即证明本命题.

在阿贝尔群中，所有内自同构缩减成恒等映射，因而只有外自同构是可能的非平凡自同构. 下面的简单例子可以用来作具体说明.

(1) 无限循环群 $C=\mathrm{gp}\{x\}$. 只要 $x\alpha$ 知道，比如说，$x\alpha=x^s$，此处 s 是一整数，则任一自同构 α 就决定了. 假如 x^k 是 C 的任一元素，那么 $x^k\alpha=(x\alpha)^k=x^{ks}$. 因而象群是 $C\alpha=\mathrm{gp}\{x^s\}$. 但是，对于一个自同构，$C\alpha=C$，因而我们必须有 $s=1$ 或 $s=-1$. 两种情况都是可能的，第一种情况是恒等映射. 因而 C 恰好有两个自同构.

(2) 有限循环群 $C_m=\mathrm{gp}\{x,x^m=1\}$. 象前面一样，只有 $x\alpha=x^s$ 需要规定. 在任一自同构下，元素的阶保持不变. 因而 x^s 一定是 m 阶的，而当且仅当 $(s,m)=1$ 时这才会发生（见 § 5，命题 2）. 于是每选一个这样的 s 导致一个自同构. 因而 C_m 有 $\phi(m)$ 个自同构，此处 $\phi(m)$ 是 § 3 中定义的欧拉函数.

(3) 四群 $V=\mathrm{gp}\{a,b;\ a^2=b^2=1,\ ab=ba\}$. 这群有三个 2 阶元素，它们只能在 α 下置换. 结果是 6 个置换各决定一个自同构. 因为，假如这三个二阶元素以 x,y,z 表示（在任一排列中），那么 $xy=z$. 所以假如 $x\alpha=x',y\alpha=y',z\alpha=z'$，我们将有 $x'y'=z'$. 即 V 具有六个自同构，即 $A(V)\cong S_3$（见 § 7）.

假如 α 是 G 的一个自同构，我们能够研究它在 G 的子群 H 上的效果. 在各种情况下，H 在 α 下的象是 G 的子群 $H\alpha$. 假如

$$H\alpha=H \tag{3.50}$$

成立（作为子集间的等式），那么我们说 H 在 α 下是不变的. 例如 H 在 G 中是正规的当且仅当在所有内自同构中它是不变的. 在那种情况下，对每一 $t\in G$，映射 $H\to t^{-1}Ht$ 是 H 的自同构.

一个子群 H 如果在所有自同构下不变就称为**特征子群**. 当

然，所有特征子群都是正规的．例如，中心Z是特征子群．因为假如$t\in Z$，那么对所有$x\in G$，$tx=xt$成立．因而，对任一$\alpha\in A(G)$，$(t\alpha)(x\alpha)=(x\alpha)(t\alpha)$；但是因为$\alpha$是满的，可以使$x\alpha$等于任一元素$y\in G$．因而对于所有的$y\in G$，$(t\alpha)y=y(t\alpha)$成立，即

$$Z\alpha\subset Z.$$

用α^{-1}代α，我们得到相反的不等式，所以$Z\alpha=Z$。

我们以证明下面的定理来结束本节．

命题 13 *假设N是G的正规子群及H是N的特征子群，那么H在G中是正规的．*

证明 设$t\in G$．那么，象我们刚才所说的那样，在(3.47)中定义的映射τ是N的自同构．因此，因为H在N中是特征的，所以我们有$H\tau=H$。因而$t^{-1}Ht=H$，即H在G中是正规的．

习 题

(1) 证明共轭元素具有相同的阶．

(2) 由互逆元素生成的两个类(a)与$(a)^{-1}$称为互逆类．证明(i) 互逆类含有相同个数的元素．(ii) 偶阶群除含有单位元素的类外至少包含一个类，它等于它的互逆类．

(3) 设$G=GL(n,F)$(见§3例(iv))，当$n\geqslant 2$及F是无限域，证明G的中心由所有单位矩阵的纯量倍组成．

(4) 找出8阶的二面体群(§14，表(xi))的中心Z，决定G/Z的结构．

(5) 证明在一域上$n\times n$非奇异上三角矩阵的集$T=\{t=(t_{ij})\mid t_{ij}=0$假如$i>j, t_{ii}\neq 0\}$在矩阵乘法下形成一个群．证明$t_{ii}=1\ (i=1,2,\cdots,n)$的子集$E$是$T$的正规子群，且$T/E\cong D$，此处$D$是非奇异对角矩阵集．

(6) 证明假如H是G的子群，那么与H共轭的子群个数等于$[G:N(H)]$．

(7) 设N是G的正规子群，N具有有限指数n．给出一元素$t\in G$，设h是使得$t^h\in N$的最小的正整数．证明$h\mid n$，还证明，假如t的阶r是有限的，那么$h\mid r$．

(8) 假如 a 与 b 是某一群的元素，使得它们的换位子 $c=[a,b]$ 与 a 及 b 两元素交换．证明假如 k 是一正整数．则

(i) $a^k b = b a^k c^k$ 及 (ii) $(ab)^k = b^k a^k c^{\frac{1}{2}k(k+1)}$.

(9) 设 N 是 G 的正规子群，N 具有有限指数 n．证明假如 A 是 G 的任一子群，那么 $s=[A:A\cap N]$ 是有限的，而且 $s|n$.

(10) 找出下列群的导出群：(i) 8 阶二面体群，(ii) 四元数群.

(11) 证明 G 的正规子群的中心化子是 G 的正规子群.

(12) 证明在阿贝尔群中，映射 $x\theta = x^{-1}$ 是一个自同构.

(13) 证明 $I(G)$ 是 $A(G)$ 的正规子群.

(14) 证明 G' 是 G 的特征子群.

第四章　有限生成的阿贝尔群

§ 25. 预备知识. 本章我们将只研究阿贝尔群，此时采用加法的记号较为方便. 我们想起，阿贝尔群的所有子群都是正规的. 假如 $H \leqslant G$，则商群 G/H 由陪集 $H+x(x\in G)$ 构成. 群 G 称为**有限生成的**，缩写为 f. g.，假如 G 中存在有限个元素 $u_1, u_2, \cdots, u_n$，称为**生成元**，使得

$$G=\mathrm{gp}\{u_1, u_2, \cdots, u_n\}.$$

那么 G 的每一元素 x 是这些生成元中的某些元素或它们的负元素(逆元素)中的某些元素在任意次序下的有限和，重复是允许的. 可是，由于交换律，我们能够合并相同生成元的项，于是我们能写成

$$x=a_1u_1+a_2u_2+\cdots+a_nu_n, \tag{4.1}$$

此处 a_2 是整数(正、负整数或零). 反之，对于任意选择的整数系数，(4.1)表示 G 的一个元素. 但是没有假定生成元是不多余的，即使是多余的，它们也可能满足非平凡关系

$$c_1u_1+c_2u_2+\cdots+c_nu_n=0 \tag{4.2}$$

上式中不是所有的系数都是零. 由于分数系数是不允许的，我们通常不能从(4.2)中解出某一个 u，使它可用其他的 u 表示出来.

以后，我们经常有必要改变一组给定的生成元，因此研究两组元素都能用作同一阿贝尔群的生成元的条件是重要的. 假设

$$G=\mathrm{gp}\{u_1, u_2, \cdots, u_n\}=\mathrm{gp}\{v_1, v_2, \cdots, v_m\}. \tag{4.3}$$

为了(4.3)能够成立，必要和充分的条件是每一 u 可用 v 表出，反之每一 v 可用 u 表出. 因而我们有以下形式的方程组

$$\left.\begin{array}{l} u_i=\sum\limits_{j=1}^{m} p_{ij}v_j(i=1,2,\cdots,n) \\ v_j=\sum\limits_{k=1}^{n} q_{jk}u_k(j=1,2,\cdots,m) \end{array}\right\} \quad (4.4)$$

此处矩阵 $\boldsymbol{p}=(p_{ij})$ 及 $\boldsymbol{q}=(q_{jk})$ 具有整数元素或者，更简单地，是**整数矩阵**．我们把方程组(4.4)叫做将生成元组 $u_1,u_2,\cdots,u_n$ 变到生成元组 $v_1,v_2,\cdots,v_m$ 的**变换**．

下面这些形式的生成元变换是最普通的．

(α) 生成元可以用任何方式置换．

(β) 假如 $i\neq j$，生成元 u_i 可以用 u_i+hu_j 代替，此处 h 是任意整数，其他的生成元保持不变．

(γ) 任一生成元 u_i 可以用 $-u_i$ 代替．

(δ) 假如生成元是零，它就可以略去．

(α)，(β) 与 (γ) 的运算称为初等变换．让我们验算(β) 确实满足(4.4)．为了简便起见，假设 $i=1,j=2$．因此我们有变换

$$v_1=u_1+hu_2, v_2=u_2,\cdots,v_n=u_n,$$

下列方程给出这个变换的逆：

$$u_1=v_1-hv_2, u_2=v_2,\cdots,u_n=v_n.$$

上面列举的运算可以反复应用，直到我们得到一组便于我们使用的生成元为止．

有个小技巧值得在这里提出．为了证明 G 的子集 X 形成一个子群只要证明下面的结论就足够了．即当 x 与 y 属于 X，那么

$$x-y\in X.$$

因为假如这是真的，我们可以取 $x=y$ 而得出 $0\in X$．还有，选 $x=0$，我们得出 $-y\in X$．最后，用 $-y$ 代 y 我们得出 $x+y\in X$．因而验证了所有有关 X 是 G 的子群的条件(见 § 9)．

我们将限于讨论有限生成的阿贝尔群．我们的目的是完整地

描述这类群的所有可能形式(直到同构).类似直积的概念(§ **13**),将G分成某些子群的**直和**可以达到这个目的. 直和写为

$$G=H\oplus K. \tag{4.5}$$

我们在这里讨论内直和. 因而(4.5)意味着存在G的子群H与K具有以下性质:

G的元素由所有可能的和

$$x=u+v \tag{4.6}$$

组成,此处u与v各自独立地遍历H与K,以及这个表示是唯一的. 因而假如

$$u_1+v_1=u_2+v_2, \tag{4.7}$$

此处$u_1,u_2\in H$及$v_1,v_2\in K$,那么$u_1=u_2$,$v_1=v_2$. 特别,假如$u_0+v_0=0$,此处$u_0\in H$,$v_0\in K$,那么$u_0=v_0=0$. 反之,这个性质保证了(4.6)的唯一性,因为(4.7)蕴含$(u_1-u_2)+(v_1-v_2)=0$,因而$u_1=u_2$、$v_1=v_2$.还有,为了证明(4.5),只要证明下面两点就足够了:

(i) $G=H+K$ 及 (ii) $H\cap K=\{0\}$.

当H与K是阶互素的有限群时,第二个条件肯定满足.

当G表成几个子群的直和时,我们使用记号

$$G=\sum_{i=1}^{r}\oplus H_i=H_1\oplus H_2\oplus\cdots\oplus H_r. \tag{4.8}$$

我们想起直和的结构(直到同构)是既交换又结合的.事实上(4.8)说明G与元素都是r-重元$(u_1,u_2,\cdots,u_r)$的群同构,此处u_i遍历H_i,而元素的合成分别由每一分量的合成来实现.

例如,假如

(i) $G=H_1+H_2+\cdots+H_r$

及

(ii) H_i及$H_j(i\neq j)$的阶是互素的,

则(4.8)肯定成立. 因为在这情况下,显然

$$H_i\cap H_1+\cdots+H_{i-1}+H_{i+1}+\cdots+H_r=\{0\}.$$

§ 26. 有限生成的自由阿贝尔群. 本节我们研究有限生成的阿贝尔群.

$$F=\mathrm{gp}\{u_1,u_2,\cdots,u_n\},\tag{4.9}$$

在 F 中生成元不满足任意非平凡关系,即我们假定

$$c_1u_1+c_2u_2+\cdots+c_nu_n=0\tag{4.10}$$

总是意味 $c_1=c_2=\cdots=c_n=0$. 假如这样的生成元组存在,我们称 F 为**自由阿贝尔群**. 更精确地说,F 由 $u_1,u_2,\cdots,u_n$ **自由生成**. 这样的生成元组称为自由生成元组,我们用下面的记号表示

$$F=\langle u_1,u_2,\cdots,u_n\rangle.\tag{4.11}$$

因而(4.11)等于说 F 的元素唯一地表示成下面的形式:

$$x=a_1u_1+a_2u_2+\cdots+a_nu_n,\quad 此处\ a_i\ 是任意整数.\tag{4.12}$$

显然,在自由阿贝尔群中,除零之外,所有的元素都是无限阶的. 因为假如 $x\neq0$ 及 $h>0$, 等式 $hx=0$ 立即导致一个生成元的非平凡关系,特别,每一生成元是无限阶的,(4.11)等价于

$$F=\mathrm{gp}\{u_1\}\oplus\mathrm{gp}\{u_2\}\oplus\cdots\oplus\mathrm{gp}\{u_n\},\tag{4.13}$$

即 F 是 n 个无限循环群的直和.

容易给出 n 个自由生成元的自由阿贝尔群的例子: 设 Z^n 是所有 n-重元 $x=[a_1,a_2,\cdots,a_n]$的集合,此处 $a_1,a_2,\cdots,a_n$ 独立地遍历所有整数. Z^n中的合成规则定义为按分量相加,因而使 Z^n 成为一个阿贝尔群. 特殊的 n-重元

$$u_1=[1,0,\cdots,0],\ u_2=[0,1,\cdots,0],\ \cdots,u_n=[0,0,\cdots,1]$$

生成 Z^n. 因为,对于任一$x\in Z^n$,

$$x=a_1u_1+a_2u_2+\cdots+a_nu_n.$$

此外,这些生成元是自由的,因为

$$c_1u_1+c_2u_2+\cdots+c_nu_n=[c_1,c_2,\cdots,c_n]=0$$

意味 $c_1=c_2=\cdots=c_n=0$.

接着我们要考查不同生成元组之间的联系．假如

$$F=\langle u_1,u_2,\cdots,u_n\rangle=\langle v_1,v_2,\cdots,v_m\rangle, \tag{4.14}$$

两组生成元由方程(4.4)联系．但是因为生成元是自由的，这时，我们有更精确的结果．在(4.4)中消去 v_j 得到

$$u_i=\sum_{j=1}^{m}\sum_{k=1}^{n}p_{ij}q_{jk}u_k \quad (i=1,2,\cdots,n).$$

这将是 u 之间的非平凡关系，除非等式两边对应的系数一致．因此我们有

$$\sum_{j=1}^{m}p_{ij}q_{jk}=\delta_{ik} \quad (i,k=1,2,\cdots,n),$$

此处 $\delta_{ik}=0$ 假如 $i\neq k$，而 $\delta_{ii}=1$．或者用矩阵符号表示成

$$\boldsymbol{pq}=\boldsymbol{i}_n, \tag{4.15}$$

此处 $\boldsymbol{i}_n$ 是 n 阶单位矩阵．相似地，消去 u，我们有

$$\boldsymbol{qp}=\boldsymbol{i}_m. \tag{4.16}$$

具有一些线性代数知识的读者将不难从(4.15)和(4.16)推导出 $m=n$．或者，我们能够利用计算(4.15)及(4.16)中的对角线元素的和来验证这事实，即

$$\sum_{i=1}^{n}\sum_{j=1}^{m}p_{ij}q_{ji}=n, \quad \sum_{j=1}^{m}\sum_{i=1}^{n}q_{ji}p_{ij}=m.$$

因为这两式的左边相等，那么 $m=n$．因而自由生成元的个数对于 F 是不变的，即每一组自由生成元的个数都是一样的．这个数称为 F 的**秩**．此外，两个有限生成自由阿贝尔群是同构的当且仅当它们有相同的秩．因为假如秩是 n，那么这群与(4.13)所表示的群同构，或者等价地，与所有 n-重整数的群同构．

取(4.15)或(4.16)中的行列式，我们得出

$$(\det\boldsymbol{p})(\det\boldsymbol{q})=1. \tag{4.17}$$

但是 p 与 q 的元素是整数，它们的行列式因此也是整数. 因而我们从(4.17)推导出 $\det p=\det q=\pm 1$，即 p 与 q 是幺模矩阵，因而具有整数矩阵为逆元素(见§3，例(iv)，(c)). 因而从一组自由生成元到另一组自由生成元的变换是幺模变换

$$u_i=\sum_{j=1}^{n} p_{ij}v_j (j=1,2,\cdots,n). \tag{4.18}$$

显然，为了这一目的可以用任一幺模矩阵 p. 因为用下方程给出变换(4.18)的逆

$$v_j=\sum_{k=1}^{n} q_{jk}u_k (j=1,\cdots,n) \tag{4.19}$$

此处 $q=p^{-1}$ 还是整数矩阵，因而验证了(4.4)式.

在§25中所描写的(α)(β)与(γ)运算是幺模变换的简单例子. 当相继实施几个这样的运算，对应的矩阵就相乘.

一组不全是零的整数 $a_1,a_2,\cdots,a_n$ 的最大公约数(HCF) 写为

$$(a_1,a_2,\cdots,a_n).$$

根据定义，这是正整数. 特别，当 $(a_1,a_2,\cdots,a_n)=1$ 时，我们说这些整数互素. 显然，在幺模矩阵中形成一行或一列的元素必然互素. 因为假如这矩阵的行列式相对一行(或一列)展开，显然，这行列式可以被这一行(或这一列)的最大公约数除尽. 可是，由假设，行列式等于±1，从而最大公约数只能等于1. 因而假如新的一组自由生成元由(4.19)引入，那么，每一新生成元是原来的生成元带有互素系数的线性组合. 下面的命题证明了这个事实的部分逆命题.

命题*14　设 $F=\langle u_1,u_2,\cdots,u_n\rangle$. 假定 $v=b_1u_1+b_2u_2+\cdots$

* 见 R.Rado, 'A proof of the basis theorem for finitely generated Abelian groups', *Journal of the London Mathematical Society*(1951).**26**, 74-75.

$+b_nu_n$ 是 F 的元素，使得

$$(b_1,b_2,\cdots,b_n)=1, \tag{4.20}$$

那么存在 F 的元素 $v_2,v_3,\cdots,v_n$，使得

$$F=\langle v,v_2,v_3,\cdots,v_n\rangle. \tag{4.21}$$

换句话说，(4.20)是某一元素能加入到一组自由生成元内的充分必要条件.

证明　设 $s=|b_1|+|b_2|+\cdots+|b_n|$. 假如 $s=1$，那么 $v=\pm u_j$，对于某一 j. 显然，v 可以包括在一组自由生成元内. 我们于是对 s 用归纳法，同时保留改变 F 的生成元的权利直到 (4.21) 建立为止. 假如 $s>1$，至少有两个 b 不是零，因为否则$(b_1, b_2, \cdots,b_n)>1$. 不失普遍性，可以假定 $b_1\geqslant b_2>0$，因为利用置换生成元和改变它们的符号(§ 25 运算(α)与(γ))这个条件总是可以满足. 现在设

$$u_1'=u_1,\quad u_2'=u_2+u_1,\quad u_j'=u_j(j\geqslant 3),$$

显然，$F=\langle u_1',u_2',\cdots,u_n'\rangle$(运算($\beta$)). 于是对 v 的表示式变成$v=(b_1-b_2)u_1'+b_2u_2'+\cdots+b_nu_n'$. 显然，$((b_1-b_2),b_2,b_3,\cdots,b_n)=1$，但是

$$|b_1-b_2|+|b_2|+|b_3|+\cdots+|b_n|<s,$$

因而由归纳假设，v 能够包含在一组自由生成元内.

我们现在把注意力转向有限生成自由阿贝尔群 F 的子群 H. 我们可以问 H 是否也是有限生成自由阿贝尔群. 这个问题可以用下面的定理肯定地回答. 这定理对于阿贝尔群理论是十分重要的；它还证明一个更深刻的结论，即只要适当选好 F 的生成元，那么 H 的生成元可以用非常简单的方式表示出来.

定理 12　设 F 是秩为 n 的有限生成自由阿贝尔群，又设 H 是 F 的非零子群. 那么 H 是秩为 m 的有限生成自由阿贝尔群，$m\leqslant n$. 对 F 可以选取这样一组自由生成元 $v_1,v_2,\cdots,v_n$，使得

$$H=\langle h_1v_1,h_2v_2,\cdots,h_mv_m\rangle, \tag{4.22}$$

此处 $h_1, h_2, \cdots, h_m$ 是正整数，满足关系

$$h_i | h_{i+1} (i=1, 2, \cdots, m-1).$$

证明 (i)假设 F 原用自由生成元 $u_1, u_2, \cdots, u_n$ 给出. 对于 F 的每一个非零元素 $x=a_1u_1+a_2u_2+\cdots+a_nu_n$，我们将它与它关于这组生成元的系数的最大公约数联系起来，比如说

$$\delta(x)=(a_1, a_2, \cdots, a_n).$$

这个数与生成元的选择无关. 因为假如 $u_1', u_2', \cdots, u_n'$ 是另一组 F 的自由生成元，我们有 $u_i=\sum_j p_{ij}u_j'$，此处 (p_{ij}) 是一个幺模矩阵. 那么 $x=a_1'u_1'+a_2'u_2'+\cdots+a_n'u_n'$，此处 $a_j'=\sum_i a_i p_{ij}$. 因而这些 a_i 的任一公因数必能除尽所有的 a_j'，从而

$$(a_1', a_2', \cdots, a_n') \geqslant (a_1, a_2, \cdots, a_n).$$

假如我们利用矩阵 (p_{ij}) 的逆来交换两组生成元的地位，我们就能证明相反的不等式. 因而 $(a_1', a_2', \cdots, a_n')=(a_1, a_2, \cdots, a_n)$，这证明了 $\delta(x)$ 的不变性.

(ii) 在 H 的非零元素中设

$$y_1=b_1u_1+b_2u_2+\cdots+b_nu_n$$

是这样的元素，它的 δ 取最小值，比如说 $\delta(y_1)=h_1\geqslant 1$. 于是我们能写成 $y_1=h_1(c_1u_1+c_2u_2+\cdots+c_nu_n)=h_1v_1$，此处 $v_1=c_1u_1+c_2u_2+\cdots+c_nu_n$ 是 F 的元素，具有性质 $(c_1, c_2, \cdots, c_n)=1$. 由命题 14，存在元素 $v_2', v_3', \cdots, v_n'$，使得

$$F=\langle v_1, v_2', v_3', \cdots, v_n'\rangle. \tag{4.23}$$

利用这组生成元，设 $y=d_1v_1+d_2v_2'+\cdots+d_nv_n'$ 是 H 的任一元素，我们知道

$$y_1=h_1v_1\in H, \tag{4.24}$$

于是我们断定 $h_1|d_1$. 因为假如不是这样，我们能找到整数 q 与 r，使得 $d_1=qh_1+r$，此处 $0<r<h_1$，因而 $y-qy_1=rv_1+d_2v_2'+$

$\cdots+d_nv'_n$ 将是H的元素，使得 $\delta(y-qy_1)=(r,d_2,\cdots,d_n)\leqslant r<h_1$，这与 h_1 的最小性矛盾. 因而我们断定 $r=0$，即

$$y-qy_1=d_2v'_2+\cdots+d_nv'_n. \tag{4.25}$$

(iii) 对 n 用归纳法. 当 $n=1$，我们已经达到目的. 因为在这情况下，(4.25)的右边必须是零，于是 $y=qy_1=qh_1v_1$. 这等于说 $F=\langle v_1\rangle,H=\langle h_1v_1\rangle$，正象定理所断定的那样，此时 $n=m=1$. 现在假设 $n>1$，又设

$$F_1=\langle v'_2,v'_3,\cdots,v'_n\rangle,\quad H_1=H\cap F_1. \tag{4.26}$$

注意(4.25)右边属于 F_1 而左边位于H中，因而(4.25)表示 H_1 的元素. 有两个情况必须考虑：首先，假如 $H_1=\{0\}$，我们有 $y=gy_1=gh_1v_1$，于是象以前那样 $H=\langle h_1v_1\rangle$，这与(4.23)一起就证明了定理，此时 n 是任意的而 $m=1$. 其次，当 H_1 是F_1 的非零子群时，我们应用归纳假设到 F_1 与 H_1 上，因而我们能找到 F_1 的元素 $v_2,v_3,\cdots,v_n$，使得

$$F_1=\langle v_2,v_3,\cdots,v_n\rangle,H_1=\langle h_2v_2,h_3v_3,\cdots,h_mv_m\rangle, \tag{4.27}$$

此处 m 是某一整数满足 $2\leqslant m\leqslant n$ 及 $h_i|h_{i+1}$ $(i=2,3,\cdots,m-1)$. 两组 F_1 的自由生成元用下面的方程式联系：

$$v_i=\sum_j p_{ij}v'_j,\quad v'_i=\sum_j q_{ij}v_j\,(i,j=2,3,\cdots,n).$$

我们断定

$$F=\langle v_1,v_2,\cdots,v_n\rangle. \tag{4.28}$$

因为，在(4.23)中用 v 来表示 v'，我们看到 $v_1,v_2,\cdots,v_n$ 肯定生成F. 此外，这些元素是自由生成元，因为假如我们有非平凡关系

$$c_1v_1+c_2v_2+\cdots+c_nv_n=0, \tag{4.29}$$

我们注意 $c_1\neq0$，因为假如不是这样，在 $v_2,v_3,\cdots,v_n$ 之间将有一关系，这与(4.27)矛盾. 假如现在我们用 $v'_2,v'_3,\cdots,v'_n$ 在(4.29)中代替 $v_2,v_3,\cdots,v_n$，我们将在 $v_1,v'_2,v'_3,\cdots,v'_n$ 之中得到一

关系，其中 v_1 的系数是 c_1. 这与(4.23)是不相容的. 因而(4.28)得证. 结合(4.24),(4.25)与(4.27)，我们得出元素

$$h_1v_1(=y_1),h_2v_2,\cdots,h_mv_m$$

生成H. 事实上，它们是自由生成元，因为它们之间任一非平凡关系也将是 $v_1, v_2, \cdots, v_m, \cdots, v_n$ 之间的一个关系，因此与(4.28)矛盾. 因而

$$H=\langle h_1v_1,h_2v_2,\cdots,h_mv_m\rangle.$$

为了结束证明，我们还需证明 $h_1|h_2$. 因为 $y_0=h_1v_1+h_2v_2$ 是H的元素，因而由 h_1 的最小性，$\delta(y_0)=(h_1, h_2)\geqslant h_1$. 从最大公约数的定义，$(h_1, h_2)\leqslant h_1$，因此$(h_1,h_2)=h_1$，即 $h_1|h_2$.

§ 27. 有限生成的阿贝尔群. 我们现在转向讨论任意一个有限生成阿贝尔群A. 当然，所有有限阿贝尔群都属于这一类. 设

$$A=\text{gp}\{s_1, s_2, \cdots, s_n\},$$

此处允许生成元 $s_1, s_2, \cdots, s_n$ 满足非平凡关系. 我们将 A 与下面的自由阿贝尔群联系：

$$F=\langle u_1, u_2, \cdots, u_n\rangle,$$

它由 $u_1,u_2,\cdots,u_n$ 自由生成. 为了建立 A 与 F 间的联系，我们引入映射

$$\theta:F\to A,$$

θ 的定义是

$$(a_1u_1+a_2u_2+\cdots+a_nu_n)\theta\to a_1s_1+a_2s_2+\cdots+a_ns_n \tag{4.30}$$

我们留给读者去证明这容易的结论，即 θ 是同态. 显然，θ 是满的，因为A的任一元素能够在(4.30)右边出现. 设R是 θ 的核，它是F的子群. 因而F的元素 $a_1u_1+a_2u_2+\cdots+a_nu_n$ 属于R当且仅当 $a_1s_1+a_2s_2+\cdots+a_ns_n=0$，这是$A$的生成元之间的关系. 于是我们能够说，$R$的元素与被$A$的生成元所满足的关系一一对应. 第一同构定理(§21)说明

$$A \cong F/R. \tag{4.31}$$

于是我们能够用考查 F/R 来找出 A 的结构. 对于这点，由于前一节的讨论,我们已经作好充分准备. 因而，只要 $R \neq \{0\}$，我们可以这样来选择 F 的自由生成元 $v_1, v_2, \cdots, v_n$，使得

$$F = \langle v_1, v_2, \cdots, v_n \rangle,$$
$$R = \langle h_1 v_1, h_2 v_2, \cdots, h_m v_m \rangle (m \leqslant n), \tag{4.32}$$

及 $$h_i \mid h_{i+1} (i = 1, 2, \cdots, m-1).$$

作为准备,让我们考虑 $n=1$ 的情况. 此时我们必须区别三种情况：

(i) $F = \langle v \rangle, R = \{0\}$. 那么 $F/R \cong F$, A 是由 v 生成的无限循环群.

(ii) $F = \langle v \rangle, R = \langle hv \rangle$,此处 $h \geqslant 2$. 那么 $F/R \cong C_h$, C_h 是 h 阶循环群.

(iii) $F = \langle v \rangle, R = \langle v \rangle (h=1)$. 那么 $F/R \cong \{0\}$, 因为 $F = R$.

一般情况下同样的特点也会出现. 需要对三种形式的生成元改用不同的符号. 假如 $r = n - m > 0$, F 中存在 r 个不在 R 中出现的生成元，这些生成元将以 $x_1, x_2, \cdots, x_r$ 表示. 假如 $h_1 = h_2 = \cdots = h_l = 1$，相应的生成元，比如说 $z_1, z_2, \cdots, z_l$ 将既在 F 中也在 R 中出现. 假如 $n = r + l + k$，剩下的 k 个生成元对应于大于 1 的 h，为了方便起见按数值下降的次序重新排列这 k 个 h,比如说,写成 $e_1, e_2, \cdots, e_k$. 因而我们将写成

$$F = \langle x_1, x_2, \cdots, x_r, y_1, \cdots, y_k, z_1, z_2, \cdots, z_l \rangle, \tag{4.33}$$

$$R = \langle e_1 y_1, e_2 y_2, \cdots, e_k y_k, z_1, z_2, \cdots, z_l \rangle, \tag{4.34}$$

此处 $e_{\kappa+1} \mid e_\kappa (k = 1, 2, \cdots, k-1)$, $n = r + k + l$, $m = k + l$. 当其中一种形式的生成元不出现时,上面的式子显然随之修正.

假如 $x \in F$,设 $\bar{x} = x + R$ 是 x 在自然满同态 $F \to F/R$ 下的

象. 特别,依次考虑F的生成元,我们得出(i)$\bar{x}_\rho(\rho=1,2,\cdots,r)$是无限阶的元素,因为没有$x_\rho$的倍数位于$R$中;(ii) $\bar{y}_\kappa$是e_κ阶的($\kappa=1,2,\cdots,k$);(iii)$\bar{z}_\lambda(\lambda=1,2,\cdots,l)$是$F/R$的零元素$\bar{0}$,因为$z_\lambda\in R$. 现在$F$的一般元素可以用下面形式表示:

$$x=\sum_{\rho=1}^{r} a_\rho x_\rho+\sum_{\kappa=1}^{k} b_\kappa y_\kappa+\sum_{\lambda=1}^{l} c_\lambda z_\lambda,$$

从而F/R的典型元素成为

$$\bar{x}=\sum_{\rho=1}^{r} a_\rho \bar{x}_\rho+\sum_{\kappa=1}^{k} b_\kappa \bar{y}_\kappa. \tag{4.35}$$

因而F/R由$\bar{x}_1,\cdots,\bar{x}_r$, $\bar{y}_1,\cdots,\bar{y}_k$所生成. 而且,我们断定事实上

$$F/R=\mathrm{gp}\{\bar{x}_1\}\oplus\cdots\oplus\mathrm{gp}\{\bar{x}_r\}\oplus\mathrm{gp}\{\bar{y}_1\}\oplus\cdots\oplus\mathrm{gp}\{\bar{y}_k\}. \tag{4.36}$$

即我们断定(4.35)的右边等于零当且仅当其中每项是零. 假设

$$\sum_{\rho=1}^{r} a_\rho \bar{x}_\rho+\sum_{\kappa=1}^{k} b_\kappa \bar{y}_\kappa=\bar{0}.$$

这意味

$$\sum_{\rho=1}^{r} a_\rho x_\rho+\sum_{\kappa=1}^{k} b_\kappa y_\kappa\in R.$$

看一下(4.34)就知道$a_\rho=0(\rho=1,2,\cdots,r)$,因为$x_\rho$不在$R$中出现. 而且$b_\kappa$一定能被$e_\kappa$除尽($\kappa=1,2,\cdots,k$),比如说$b_\kappa=d_\kappa e_\kappa$. 因而$b_\kappa\bar{y}_\kappa=d_\kappa e_\kappa\bar{y}_\kappa=\bar{0}$, 因为$e_\kappa\bar{y}_\kappa=\bar{0}$. 这证明了(4.36). 因为由(4.31)我们可以将所给的群A与F/R等同,所以我们已经证明了下面的基本定理.

定理 13(有限生成阿贝尔群的基本定理) 每一个有限生成阿贝尔群A是循环群的直和,包含$r(\geqslant 0)$个无限循环群及$k(\geqslant 0)$个有限循环群;因而

$$A=\mathrm{gp}\{t_1\}\oplus\cdots\oplus\mathrm{gp}\{t_r\}\oplus\mathrm{gp}\{w_1\}\oplus\cdots\oplus\mathrm{gp}\{w_k\}, \quad (4.37)$$

此处 $t_\rho(\rho=1,2,\cdots,r)$是无限阶的，而$w_\kappa(\kappa=1,2,\cdots,k)$是有限阶 $e_\kappa(\geqslant 2)$的，此外

$$e_{\kappa+1}|e_\kappa \quad (\kappa=1,2,\cdots,k-1). \quad (4.38)$$

这定理有效地解决了描写所有有限生成阿贝尔群结构的问题. 出现在直和分解式(4.37)中的生成元称为 A 的**基**. 重复说一遍，它们不象向量空间的基元素那样，是"自由的"或"独立的"，而是具有这样的性质，即在非平凡关系式中每项都是零.

当 $r=0$，群 A 是有限的而$|A|=e_1e_2\cdots e_k$；在另一个极端情况，即当 $k=0$ 时，A 是自由阿贝尔群. 不论 A 是否是自由的，自由生成元的个数 r 称为 A 的**秩**.

在定理 13 中所描述的分解式称为A的**标准形**，只要数学对象的结构表示成简单的，本质上唯一的形式，我们就用这个有点含糊的名词. 到目前为止放在一边的唯一性问题将在下节讨论.

§ 28. 不变量与初等因子. 刚才提到的唯一性问题明确地说就是：

定理 14 设 A 是有限生成阿贝尔群，又假设

$$A=\mathrm{gp}\{x_1\}\oplus\cdots\oplus\mathrm{gp}\{x_r\}\oplus\mathrm{gp}\{u_1\}\oplus\cdots\oplus\mathrm{gp}\{u_k\} \quad (4.39)$$

$$=\mathrm{gp}\{y_1\}\oplus\cdots\oplus\mathrm{gp}\{y_s\}\oplus\mathrm{gp}\{v_1\}\oplus\cdots\oplus\mathrm{gp}\{v_l\}, \quad (4.40)$$

此处 $x_\rho(\rho=1,2,\cdots,r)$及 $y_\sigma(\sigma=1,2,\cdots,s)$是无限阶元素，又 u_k 的阶$|u_\kappa|=d_\kappa(\kappa=1,2,\cdots,k)$，$d_{\kappa+1}|d_\kappa$，$v_\lambda$ 的阶$|v_\lambda|=e_\lambda$ ($\lambda=1,2,\cdots,l$)，$e_{\lambda+1}|e_\lambda$. 那么(i) $r=s$，(ii) $k=l$，$d_\kappa=e_\kappa$ ($\kappa=1,2,\cdots,k$).

这定理的证明要占这节的大部分，我们将分几步进行.

(i) 设 T 是 A 的有限阶元素的集合，假如 $u,v\in T$，则存在整数m和 n 使得 $mu=nv=0$. 因而 $mn(u-v)=0$. 所以$u-v\in T$. 这证明 T 是子群(见§25). 这个群称为 A 的**挠子群**，这是一个从拓扑借来的名词，当然 T 是由 A 决定的，即它不依赖基元素的选

择. 现在,

$$X=\sum_{\rho=1}^{r}\oplus \mathrm{gp}\{x_\rho\} \text{ 及 } Y=\sum_{\sigma=1}^{s}\oplus \mathrm{gp}\{y_\sigma\}$$

分别是秩为 r 和 s 的自由阿贝尔群. (4.39)与 (4.40) 的假设意味

$$A=X\oplus T=Y\oplus T. \tag{4.41}$$

因为显然挠群不能包含任一无限阶生成元, 而必定包含所有有限阶的生成元. 从(4.41)我们推导出 $A/T\cong X, A/T\cong Y$, 从而 $X\cong Y$. 但是一个自由阿贝尔群的秩是不变量(§ 26), 因而 $r=s$, 于是定理 14 的第一部分已经证明.

(ii) 从现在起我们将只讨论有限阿贝尔群. 即我们忽略 (4.39)及(4.40)中的无限生成元. 我们先从 A是有限阿贝尔 p-群的特殊情况着手, 即我们假设 $|A|=p^m$, 此处 p 是素数, m 是一正整数. 那么每一元素的阶是 p 的幂, 特别我们令

$$|u_\kappa|=d_\kappa=p^{\delta_\kappa}(\kappa=1,2,\cdots,k),$$
$$|v_\lambda|=e_\lambda=p^{\varepsilon_\lambda}(\lambda=1,2,\cdots,l).$$

条件 $d_{\kappa+1}|d_\kappa$ 等价于 $\delta_{\kappa+1}\leqslant\delta_\kappa$; 相似地 $\varepsilon_{\lambda+1}\leqslant\varepsilon_\lambda$. 因此, 对于 p-群来说, 定理 14 就是下面的结果.

定理 15 设 A 是有限阿贝尔 p-群, 假设

$$A=\sum_{\kappa=1}^{k}\oplus \mathrm{gp}\{u_\kappa\}=\sum_{\lambda=1}^{l}\oplus \mathrm{gp}\{v_\lambda\}, \tag{4.42}$$

此处 $|u_\kappa|=p^{\delta_\kappa}(\kappa=1,2,\cdots,k)$, $|v_\lambda|=p^{\varepsilon_\lambda}$ $(\lambda=1,2,\cdots,l)$ 及 $\delta_1\geqslant\delta_2\geqslant\cdots\geqslant\delta_k, \varepsilon_1\geqslant\varepsilon_2\geqslant\cdots\geqslant\varepsilon_l$, 那么 $k=l$ 及 $\delta_\kappa=\varepsilon_\kappa$ $(\kappa=1,2,\cdots,k)$.

证明* 假如 $|A|=p^m$, 那么比较(4.42)中的阶, 得

* 我们仿效 Marshall Hall Jr. *The Theory of Groups* (New York, 1959) p. 41的证明.

$$m=\sum_{\kappa}\delta_{\kappa}=\sum_{\lambda}\varepsilon_{\lambda}.$$

当$m=1$，这定理是显而易见的，因此我们对m作归纳进行证明.

设A_p是满足$px=0$的元素的集合. 因为$p(x-y)=px-py$，那么A_p是A的子群(可能等于A). 决定A_p的阶是不难的. 因为设$x\in A_p$，对A采用基$u_1,u_2,\cdots,u_k$，我们有

$$x=\sum_{i=1}^{k}a_iu_i.$$

此处可假定$0\leqslant a_i<p^{\delta_i}$，因为$|u_i|=p^{\delta_i}$. 于是假如$px=0$，那么对每一$i$，$pa_iu_i=0$，因而$p^{\delta_i}|pa_i$，因而$a_i=b_ip^{\delta_i-1}$，此处$b_i$必须满足$0\leqslant b_i<p$.因而对于某一固定$i$，$b_i$恰好存在$p$个可能的值，因而$a_i$也恰好存在$p$个可能的值使得$px=0$. 这证明了$|A_p|=p^k$. 在(4.42)中采用第二组基，我们类似地得出$|A_p|=p^l$. 但是$A_p$与基无关. 因此$k=l$，正象所要求的那样.

其次，我们定义集A^p为A的所有那些元素x的集，它们是另一元素的p倍(p次幂的加法类似). 易于验证A^p事实上是子群，因为假如$x=px'$，$y=py'$，那么$x-y=p(x'-y')$.假如我们简单地用p来乘A的基元素作为A^p的基元素，那么我们就得到A^p到循环群的直和分解. 但是必须注意这个运算“杀死”所有的p阶元素. 因而设

$$\delta_1\geqslant\delta_2\geqslant\cdots\geqslant\delta_K>1,\delta_{K+1}=\delta_{K+2}=\cdots=\delta_k=1$$

此处K是某一整数满足$0\leqslant K\leqslant k$，那么

$$A^p=\sum_{i=1}^{K}\oplus\mathrm{gp}\{pu_i\}\text{及}|pu_i|=p^{\delta_i-1}.$$

相似地，假如$\varepsilon_1\geqslant\varepsilon_2\geqslant\cdots\geqslant\varepsilon_L>1,\varepsilon_{L+1}=\varepsilon_{L+2}=\cdots=\varepsilon_k=1$，我们能写

$$A^p = \sum_{j=1}^{L} \oplus \mathrm{gp}\{pv_j\},$$

此处$|pv_j| = p^{\varepsilon_j - 1}$. 当$K=0$时,$A$的所有元素都是$p$阶的,从而$A^p = \{0\}$. 在那种情况下也有$L=0$,因为$A^p$不依赖基.今后,我们将假定$K>0$. 显然,$|A^p|<A$,于是我们应用归纳法假设到$A^p$上. 因而我们断定$K=L$及$\delta_i - 1 = \varepsilon_i - 1$即$\delta_i = \varepsilon_i (i=1,2,\cdots,K)$. 既然其余的$\delta$及$\varepsilon$都等于1,定理就证完了.

阿贝尔p-群A的不变量

$$p^{\delta_1}, p^{\delta_2}, \cdots, p^{\delta_k} \tag{4.43}$$

也称为A的**初等因子**. 因而两个阿贝尔p-群同构当且仅当它们具有相同的按某种次序排列的初等因子.当p的值略而不提时,只要说出(4.43)中的指数就够了.于是我们说A是$(\delta_1, \delta_2, \cdots, \delta_k)$**型**. 特别,假如$A$是$(1,1,\cdots,1)$型时,它称为初等阿贝尔$p$-群.

(iii) 下一步在于把任一有限阿贝尔群分解成p-群的和. 我们从一引理着手,它是关于单个循环子群的,而且,在它的乘法说法中,也可以适用于非阿贝尔群(见第一章习题8).

引理 设w是mn阶的元素,此处$(m,n)=1$,那么

$$\mathrm{gp}\{w\} = \mathrm{gp}\{nw\} \oplus \mathrm{gp}\{mw\}. \tag{4.44}$$

证明 元素$u=nw$,及$v=mw$分别是m与n阶的,令$W=\mathrm{gp}\{w\}, U=\mathrm{gp}\{u\}, V=\mathrm{gp}\{v\}$. 我们断定

$$W = U \oplus V. \tag{4.45}$$

因为$(m,n)=1$,存在整数a与b使$an+bm=1$,因而

$$w = (an+bm)w = a(nw) + b(mw) = au + bv,$$

这证明$w \in U+V$.但是w生成W,从而$W \subset U+V$.因为$U \subset W$及$V \subset W$,我们相反地有$U+V \subset W$. 因此$W=U+V$. 为了证明这和是直和,我们注意$U \cap V = \{0\}$,因为U与V是阶互素的群.

结论(4.44)可以推广到更多的项,特别设

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t},$$

此处$p_1,p_2,\cdots,p_t$是不同的素数,那么

$$\mathrm{gp}\{w\}=\sum_{\tau=1}^{t}\mathrm{gp}\{w_\tau\},\qquad(4.46)$$

此处$w_\tau=(m/p_\tau^{\alpha_\tau})w$是$p_\tau^{\alpha_\tau}$阶. 当某些$\alpha$是零时,公式(4.46)仍旧可以用. 对应的和简化到零群,于是可以略去.

设p是一素数,又设P是A中阶为p的幂的元素的集,即这些元素满足形式为$p^\mu x=0$ ($\mu\geqslant 0$)的方程. 显然,P是子群,因为假如$p^\mu x=p^\nu y=0$,那么$p^{\mu+\nu}(x-y)=0$. 假如p不能整除$|A|$,那么$P=\{0\}$. 我们称P为A的**p-准素分支**. 下面,我们证明当$|A|$可被一个以上素数除尽时,准素分支给出一个A的分解式.

定理 16 *设$|A|=p_1^{\nu_1}p_2^{\nu_2}\cdots p_n^{\nu_n}$,又设$P_i$是$A$的$p_i$-准素分支,那么*

$$A=P_1\oplus P_2\oplus\cdots\oplus P_n.\qquad(4.47)$$

证明 假如w是A的任一元素,那么(4.46)指出$w\in P_1+P_2+\cdots+P_n$因此$A\subset P_1+P_2+\cdots+P_n$.反之,每一$P_i$包含在$A$中,从而$A=P_1+P_2+\cdots+P_n$. 此外,这和是直和,因为这些项具有互素的阶(见§13,(3),)分解式(4.47)在下列意义上是唯一的,设

$$A=P_1^*\oplus P_2^*\oplus\cdots\oplus P_n^*,\qquad(4.47)'$$

此处P_i^*是阿贝尔p_i-群($i=1,2,\cdots,n$). 那么$P_i^*=P_i$. 因为设$|P_i^*|=p_i^{\mu_i}$;计算$(4.47)'$两边群的阶,我们得出$|A|=\prod_i p_i^{\mu_i}$. 从而由于$|A|$的素数分解的唯一性得出$\mu_i=\nu_i$. 因而$|P_i^*|=|P_i|$. 因为由P_i的定义,P_i^*的每一元素位于P_i中,即$P_i^*\subset P_i$. 既然这两个群具有相同的阶,我们断定$P_i^*=P_i$.

(iv) 最后,我们回到定理14的证明,保留定理16中的符号,已经给出

$$A=\sum_{\kappa=1}^{k}\oplus \mathrm{gp}\{u_\kappa\}, |u_\kappa|=d_\kappa \quad d_{\kappa+1}|d_\kappa. \tag{4.48}$$

证明的思路是把每项分解成它的准素分支，因此得到$P_1, P_2, \cdots, P_n$的初等因子，它们的唯一性已在定理 15 中证明过. 设

$$d_\kappa=\prod_{i=1}^{n} p_i^{\delta_{\kappa i}} \qquad (\kappa=1,2,\cdots,k), \tag{4.49}$$

此处$\delta_{\kappa i}\geqslant 0$ 及$\delta_{\kappa+1,i}\leqslant\delta_{\kappa i}$. 依次应用(4.46)到每一$u_\kappa$, 我们能写

$$\mathrm{gp}\{u_\kappa\}=\sum_{i=1}^{n}\mathrm{gp}\{u_{\kappa i}\},$$

此处$|u_{\kappa i}|=p_i^{\delta_{\kappa i}}$，因而我们能将$A$表示成$p$-群的二重和，即

$$A=\sum_{\kappa=1}^{k}\sum_{i=1}^{n}\oplus \mathrm{gp}\{u_{\kappa i}\}. \tag{4.50}$$

对每一固定 i ，我们得出

$$P_i=\sum_{\kappa=1}^{k}\oplus \mathrm{gp}\{u_{\kappa i}\}.$$

这指出P_i 的初等因子是下列单调下降序列中不等于 1 的项.

$$p_i^{\delta_{1i}}, p_i^{\delta_{2i}}, \cdots, p_i^{\delta_{ki}}.$$

这情况用下表总结之，在表中素数幂简单地用它们的指数来代表.

	p_1	p_2	$\cdots$	p_n
d_1	δ_{11}	δ_{12}	$\cdots$	δ_{1n}
d_2	δ_{21}	δ_{22}	$\cdots$	δ_{2n}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
d_k	δ_{k1}	δ_{k2}	$\cdots$	δ_{kn}

(4.51)

上表中的行对应 (4.49)，而各列中的非零元素分别决定P_1, $P_2, \cdots, P_n$的初等因子. 每一列中各项按数值非增的次序排列，而最后一行不全是零，因为$d_k\geqslant 2$.

现在假设我们用一组 e 来代替这组 d ，此处

$$e_\lambda=\prod_{i=1}^{n}p_i^{e_{\lambda i}}\quad(\lambda=1,2,\cdots,l).$$

定理 15 保证表中$(\delta_{\kappa i})$与$(\varepsilon_{\lambda i})$对应的列具有相同的非零项. 因为至少有一列$(\delta_{\kappa i})$具有 k 个非零项, 那么 $l\geqslant k$. 类似地, 由对称性, $k\geqslant l$. 因而 $k=l$. 于是表$(\delta_{\kappa i})$与$(\varepsilon_{\lambda i})$是同样的. 这便结束了定理 14 的证明. 整数$d_1,d_2,\cdots,d_k$称为$A$的**不变量**,它们总是假定满足可除性条件$d_{\kappa+1}|d_\kappa$, A的**初等因子**是准素分支$P_i(i=1,2,\cdots,n)$的初等因子的集合. 前面的讨论指出不变量与初等因子是互相决定的,它们都完全地描写了A的结构,因此规定不变量或者规定初等因子我们都可以得出一切有限生成阿贝尔群 (在同构的意义上). 后者导致分解式 (4.50), 它含有最多的循环群项,而前者得出具有最少的项的分解式(4.48).

例 1　找出初等因子是 $2^3,2,2,3,3$ 的群的不变量. (4.51) 表成为

	2	3
d_1	3	1
d_2	1	1
d_3	1	0

从而 $d_1=2^3\times3=24$, $d_2=2\times3=6$, $d_3=2$. 群的阶是

$$|A|=24\times6\times2=2^5\times3^2=288.$$

下一个例子说明如何能将循环群的直和化为对应于初等因子或不变量的标准形.

例 2　找出群A的初等因子和不变量.

$$A=C_{30}\oplus C_{12}.$$

这不是标准形,因为 $12\nmid30$. 首先, 我们将每一项分裂成阶互素的群,因而

$$A=(C_2\oplus C_3\oplus C_5)\oplus(C_4\oplus C_3).$$

集中属于同一素数的项,我们有

$$A=(C_4\oplus C_2)\oplus(C_3\oplus C_3)\oplus C_5.$$

这指出对应于素数 2,3 和 5 的初等因子分别是(4,2),(3,3)和 5．实际上，表(4.51)成为

	2	3	5
d_1	2	1	1
d_2	1	1	0

从而$d_1=2^2\times3\times5=60$，$d_2=2\times3=6$. 因而

$$A=C_{60}\oplus C_6,$$

这是显示出不变量的标准形.

§ 29. 分解的方法. 在§ 27 中我们证明了基本结论，即每一有限生成阿贝尔群A与某一循环群的直和同构. 但是证明中所用的论证，并不直接给出决定直和中各循环群的实际方法. 本节的目的是描写在具体情况中解决这个问题的系统方法.

设A用生成元和定义关系给出，因而我们假定

$$A=\mathrm{gp}\{x_1,x_2,\cdots,x_n\},$$

此处生成元$x_1,x_2,\cdots,x_n$服从N个关系式

$$\sum_{j=1}^{n}b_{ij}x_j=0\qquad(i=1,2,\cdots,N).$$

$N\times n$ 整数矩阵$B=(b_{ij})$称为**关系矩阵**. 为了将这个问题重新用公式表示出来，我们象§ 27 中那样，引入一个自由阿贝尔群

$$F=\langle u_1,u_2,\cdots,u_n\rangle \tag{4.52}$$

和一关系子群

$$R=\mathrm{gp}\{r_1,r_2,\cdots,r_N\}, \tag{4.53}$$

此处

$$r_i=\sum_{j=1}^{n}b_{ij}u_j(i=1,2,\cdots,N).$$

注意u_j由定义是F的自由生成元，而r_i只是R的生成元. 象我们在(4.31)中所看到的那样，群A于是以F/R的形式出现，当新的生成元选得使(4.32)满足时，A的结构就显露出来. 相对于这些生成元，关系矩阵具有简单的形状，即所有非对角线元素是零. 反

之，假如

$$B=\begin{bmatrix} d_1 & 0 & 0 & \cdots \\ 0 & d_2 & 0 & \cdots \\ 0 & 0 & d_3 & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix}, \tag{4.54}$$

则 A 的循环群分解也可以得到．可是除非更进一步的条件 $d_{i+1}|d_i$ 满足，这分解还不是定理 13 中所描写的标准形．为了技巧上的原因，一开始忽略这些条件，而暂时限于简化关系矩阵为对角矩阵(见上一节，例 2)是有利的．

这个问题可以从下面的表格开始讨论．

	u_1	u_2	$\cdots$	u_n
r_1	b_{11}	b_{12}	$\cdots$	b_{1n}
r_2	b_{21}	b_{22}	$\cdots$	b_{2n}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
r_N	b_{N1}	b_{N2}	$\cdots$	b_{Nn}

(4.55)

表中顶上一栏对应于 F 的生成元，而左边一栏显示 R 的生成元．因为 F 的生成元和 R 的生成元都由我们自由选择，所以我们可以应用运算(α)，(β)，(γ)，(δ)(见 § **25**)到每一组生成元上，而不会改变 F/R 的结构．对于 R，这些运算等于作用在表 (4.55) 的行上，但需要稍微注意改变 F 生成元时的影响．假设我们想用下面的变换对 F 引入新生成元：

$$u'=u_1+qu_2,\, u_2'=u_2,\, u_3'=u_3,\, \cdots,\, u_n'=u_n, \tag{4.56}$$

此处 q 是任意整数．又设

$$r=b_1u_1+b_2u_2+\cdots+b_nu_n$$

是关系子群的标准元素．关于新的生成元这个关系式变成

$$r=b_1u_1'+(b_2-qb_1)u_2'+b_3u_3'+\cdots+b_nu_n'.$$

因而(4.55)顶上一行用(4.56)代替，而在矩阵 B 中，从第二列减去

q 乘第一列，这是在列上的(β)型运算.

接着我们指出将 B 约化到对角形式(4.54)的一系列步骤.

(i) 当 $B=0$ 时，$A=F$ 是一个自由阿贝尔群，我们没有什么好说的. 因而我们将假定 $B\neq 0$. 用行的置换与列的置换，以及假如必要，改变某一行或某一列的符号，我们能够安排"主元" b_{11} 使得满足

$$b_{11}>0,\quad b_{11}\leqslant|b_{i1}|,\quad b_{11}\leqslant|b_{1j}|\,(i>1,\,j>1).$$

(ii) 可能发生这样的情况，与 b_{11} 垂直地或水平地排列在一起的所有 B 的元素可被 b_1 整除. 这时我们从另一行（列）减去第一行(列)的适当倍就能够约化这些元素为零. 这样运算之后，关系矩阵变为

$$\begin{pmatrix} b_{11} & 0 \\ 0 & B_1 \end{pmatrix}, \tag{4.57}$$

(iii) 另一方面，假如某一 b_{i1} 或 b_{1j} 不能被 b_{11} 除尽，(β) 型运算将使 b_{i1} 被它的模 b_{11} 的最小正剩余所代替. 例如，我们可以有

$$b_{i1}-qb_{11}=b'_{i1},$$

此处 $0<b'_{i1}<b_{11}$. 我们于是将 b'_{i1} 移到领头的位置，又对新的主元 b'_{i1} 重复这种约化. 因为主元的位置依次被一个下降的正整数序列所占据，所以这一过程显然在有限步骤之后一定会结束. 最后(ii)中所描写的情况一定会出现.

这样，就变成约化(4.57)这样的矩阵了，而这只要用同样的方法处理 B_1，直到得出(4.54)为止.

例 3 找出阿贝尔群 A 的不变量，A 由 a,b 与 c 所生成，服从关系式

$$3a-2b+5c=0,\quad 5a+27c=0.$$

对于关系矩阵的下列运算导出标准形.

$$\begin{bmatrix}3 & -2 & 5\\5 & 0 & 27\end{bmatrix}\xrightarrow{(1)}\begin{bmatrix}1 & -2 & 5\\5 & 0 & 27\end{bmatrix}\xrightarrow{(2)}\begin{bmatrix}1 & -2 & 5\\0 & 10 & 2\end{bmatrix}$$

$$\xrightarrow{(3)}\begin{bmatrix}1 & 0 & 0\\0 & 10 & 2\end{bmatrix}\xrightarrow{(4)}\begin{bmatrix}1 & 0 & 0\\0 & 0 & 2\end{bmatrix}\xrightarrow{(5)}\begin{bmatrix}1 & 0 & 0\\0 & 2 & 0\end{bmatrix}$$

对应不同的步骤，我们指出这些到新生成元和新关系式的变换：

(1) 生成元　$u_1=u_1', u_2=u_1'+u_2', u_3=u_3'$.

(2) 关系式　$r_1'=r_1, r_2'=r_2-5r_1$.

(3) 生成元　$u_1'=u_1''+2u_2''-5u_3'', u_2'=u_2'', u_3'=u_3''$.

(4) 生成元　$u_1''=u_1''', u_2''=u_2''', u_3''=u_3'''-5u_2'''$.

(5) 生成元　$u_1'''=v_1, u_2'''=v_3, u_3'''=v_2$.

这就完成了约化．利用§27中定理13前面的记号我们看出F/R由$\bar{v}_1$，$\bar{v}_2$，$\bar{v}_3$所生成，此处$\bar{v}_1=0, 2\bar{v}_2=0$，而$\bar{v}_3$是无限阶的．因而

$$A\cong C_2\oplus C_\infty.$$

消去中间的生成元，我们有

$$v_1=3u_1-2u_2+5u_3, v_2=-5u_1+5u_2+u_3$$

$$v_3=-u_1+u_2.$$

读者可以验算这是一个幺模变换．

当我们认为不必要记下生成元的变化时，只要对关系矩阵应用关于主元的运算直到得到对角形式为止，A的循环结构就可以显露出来．在下面的例子中，列运算就够了，第j列以$\mathbf{c}_j$表之．

例 4　找出具有生成元a,b,c,d及关系式

$$3a+9b-3c=0,\ 4a+2b-2d=0$$

的阿贝尔群的标准分解式．

关系矩阵可以约化如下：

$$\begin{bmatrix}3 & 9 & -3 & 0\\4 & 2 & 0 & -2\end{bmatrix}\longrightarrow\begin{bmatrix}3 & 9 & -3 & 0\\0 & 0 & 0 & -2\end{bmatrix}$$

$$(\mathbf{c}_1\to\mathbf{c}_1+2\mathbf{c}_4,\ \mathbf{c}_2\to\mathbf{c}_2+\mathbf{c}_4)$$

$$\rightarrow\begin{bmatrix}3 & 0 & 0 & 0\\ 0 & 0 & 0 & 2\end{bmatrix}\rightarrow\begin{bmatrix}3 & 0 & 0 & 0\\ 0 & 2 & 0 & 0\end{bmatrix}$$

$(\mathbf{c}_2\to\mathbf{c}_2-3\,\mathbf{c}_1,\ \mathbf{c}_3\to\mathbf{c}_3+\mathbf{c}_1,\ \mathbf{c}_4\to-\mathbf{c}_4)(\mathbf{c}_2\to\mathbf{c}_4,\ \mathbf{c}_4\to\mathbf{c}_2)$

由此推断只有两个生成元仍是自由的，另外两个生成元分别对应3阶与2阶的循环群．因而这群与下面的群同构

$$C_3\oplus C_2\oplus C_\infty\oplus C_\infty.$$

习　题

(1) 证明假如 $b_1,b_2,\cdots,b_n$ 是整数，且$(b_1,b_2,\cdots,b_n)=1$，那么存在幺模矩阵，它的第一行是 $b_1,b_2,\cdots,b_n$．

(2) 证明假如有限阿贝尔群的阶不可被一平方数(>1)整除，那么，这群是循环群．

(3) 证明在有限阿贝尔群中，(i)元素的最大阶等于最大的不变量，(ii)任一元素的阶都能整除这最大阶．

(4) 证明与24互素的剩余类(乘法)群是8阶初等阿贝尔群．

(5) 找出由下面的生成元和关系式所定义的阿贝尔群的初等因子和不变量：(i) $15\,a=4\,b=0$　(ii) $20\,a=6\,b=5\,c=0$．

(6) 由 a,b,c 所生成的阿贝尔群 A 具有定义关系 $3\,a+9\,b+9\,c=0$，$6\,a-12\,b=0$．将 A 表示为循环群的直和．

(7) 找出下列阿贝尔群的秩和不变量：(i) 具有生成元 a,b，及关系式 $2(a+b)=0$；(ii) 具有生成元 a,b,c,d 及关系式 $3\,a+5\,b-3\,c=0$，$4\,a+2\,b-2\,d=0$．

(8) 自由阿贝尔群 F 由 u_1,u_2,u_3 生成，而子群 R 由

$$r_1=ku_1+u_2+u_3,\quad r_2=u_1+ku_2+u_3,$$

$$r_3=u_1+u_3+ku_3$$

所生成，此处 k 是大于1的整数．求出 F 的生成元 v_1,v_2,v_3 及 R 的生成元 s_1,s_2,s_3，使得 $s_i=e_iv_i(i=1,2,3)$，而 e_1,e_2,e_3 是整数满足 $e_1|e_2|e_3$．

(9) 证明 g 阶阿贝尔群至少有一个子群，它的阶等于任一预先指定的 g 的因子．(关于阿贝尔群的拉格朗日定理的逆定理．)

(10) 验证 p^k 阶(p 是素数)的初等阿贝尔群可以看作一个由元素0,1,

$\cdots, p-1$ 组成的素域上的 k 维向量空间.

(11) 证明在 p^3 阶的初等阿贝尔群中，一个“有序的”基可以有 $p^3(p^3-1)(p^2-1)(p-1)$ 种选法.（具有相同元素但次序不同的基看作不相同）.

(12) 证明 § 27 的结果给出下面矩阵的基本定理：假如 B 是秩为 k 的 $m\times n$ 整数矩阵，那么存在分别是 m 与 n 阶的幺模矩阵 P 与 Q，使得 $PBQ=D$，此处 $D=(d_{ij})$，其中除前 k 个对角线元素外，其他所有元素都等于零，并且 $d_{11}|d_{22}|\cdots|d_{kk}$.

第五章　生成元与定义关系

§ 30. 由有限个生成元和定义关系确定的群. 在上一章我们看到，阿贝尔群的结构可以令人满意地决定，只要这个群由有限个元素生成，它们服从有限个关系. 有个问题自然地产生出来：是否有相似的理论应用到非阿贝尔群上. 这问题在 § 12 简单地提到过，我们也碰到过几个非阿贝尔群的例子，它们用生成元和关系式来描写. 象所料想的那样，缺少交换律使得情况变得复杂得多，而本书的范围只允许我们介绍这个广泛题目中最简单的概念和事实.

从一开始我们将只限于讨论这样一些群，根据假设，它们由有限个元素生成，且具有有限个关系. 我们说这样的群是由有限个生成元和定义关系确定的.

§ 31. 自由群. 我们引进非交换符号 x_1、x_2, $\cdots$, x_n，用它们形成**字**，字是一个由有限个因子构成的形式积

$$w=x_a^{\alpha}x_b^{\beta}\cdots x_r^{\rho} \tag{5.1}$$

足标 $a,b,\cdots,r$ 取自一组整数 $1,2,\cdots,n$. 因为因子不交换，所以足标可以重复. 指数 $\alpha,\beta,\cdots,\rho$ 是正整数或负整数. 我们可以把一个字当作 $x_1,x_2,\cdots,x_n$的一个函数，而相应地将 w 更明确地写作 $w(x_1,x_2,\cdots,x_n)$.

引入**空字**是方便的，空字就是因子个数是零的字，以 e 表示. 我们定义

$$x_i^0=e \quad (i=1,2,\cdots,n).$$

一个字称为**简化的**，假如它或者是空字或者是一些(5.1)形式的积，其中没有两个接连的 x 具有相同的足标.

我们来定义两个非空字 u 与 v 的乘法：写下由 u 的因子后面

跟随 v 的因子构成的形式积 p，假如 p 碰巧是简化字，我们就定义它为 uv. 假如 p 不是简化字，则假设

$$u=u_0x^\alpha,\qquad v=x^\beta v_0,$$

此处 x 的确不出现在 u_0末尾和 v_0开头，我们于是用下面的规律简化 p：

$$x^\alpha x^\beta=x^{\alpha+\beta}.\tag{5.2}$$

假如 $\alpha+\beta=0$，就去掉因子 $x^{\alpha+\beta}$，并且可以作进一步的简化和消去，这过程一直继续到得到简化的字 p_0为止. 我们于是定义

$$uv=p_0.$$

应该指出简化过程是唯一的，所以 uv 具有确定的意义. 合成规则还满足下面明显的规律

$$ue=eu=u,$$

即空字起单位元素的作用. (5.1)的逆元素是

$$w^{-1}=x_r^{-\rho}\cdots x_b^{-\beta}x_a^{-\alpha}.$$

它显然是简化字. 直接验证下面的结合律

$$(uv)w=u(vw),\tag{5.3}$$

是有点费劲的，最好分几步来实现*.

(i) 设 x 是单独一个符号，又设 u_0与 w_0为简化字（可能是空字），使得 u_0 的末尾因子与 w_0的开头因子都不是 x 的某一具有非零指数的幂. 容易看出

$$(u_0x^\alpha)(x^\beta w_0)=u_0(x^{\alpha+\beta}w_0)=(u_0x^{\alpha+\beta})w_0.$$

(ii) 假如 u 与 w 是简化字，而 x 是任一符号，那么

$$(ux^\alpha)w=u(x^\alpha w).\tag{5.4}$$

因为设

---

* 见 A.G.Kurosh, 1955, *The theory of group*, 1, p.126.（有中译本.《群论》，上册曾肯成、郝鈵新译，下册刘绍学译，高等教育出版社.）

$$u=u_0x^\pi,\qquad w=x^\phi w_0,$$

此处 u_0与 w_0象(i)中那样,而 π 与 ϕ 是 整数，它们 可以是零. 于是我们有

$$\begin{aligned}(ux^\alpha)w&=[(u_0x^\pi)x^\alpha](x^\phi w_0)=(u_0x^{\pi+\alpha})(x^\phi w_0)\\&=u_0(x^{\pi+\alpha+\phi}w_0)=u_0[x^\pi(x^{\alpha+\phi}w_0)]\\&=u_0[x^\pi(x^\alpha w)]=(u_0x^\pi)(x^\alpha w)=u(x^\alpha w).\end{aligned}$$

(iii) 最后,为了一般地证明(5.3),我们对 v 的因子个数用归纳法. v 退化到单个 x^α的情况为(5.4)所包含. 现假设

$$v=v_0x^\alpha,$$

并且结合律运用于 v_0,那么我们有

$$\begin{aligned}(uv)w&=[u(v_0x^\alpha)]w=[(uv_0)x^\alpha]w\\&=(uv_0)(x^\alpha w)=u[v_0(x^\alpha w)]\\&=u[(v_0x^\alpha)w]=u(vw).\end{aligned}$$

这完成了在一切情况下(5.3)的证明.

符号 $x_1,x_2,\cdots,x_n$的简化字的集合,连同刚才定义的合成规则,形成一个群,称为 $x_1,x_2,\cdots,x_n$上的**自由群**. 在单独一个符号 x 上的自由群是无限循环群(见 § 5). 在两个符号 x 与 y 的情况下,标准的积是

$$(xy^{-2}x)(yx)=xy^{-2}xyx$$

$$(xy^2)(y^{-1}x)=xyx$$

$$(xyx^{-1})(xy^{-1}x)=x^2.$$

作为总结,我们可以说在 $x_1,x_2,\cdots,x_n$上的自由群由所有这些符号的简化字组成,这些符号只服从平凡条件

$$x_ix_i^{-1}=x_i^{-1}x_i=e\quad(i=1,2,\cdots,n)\qquad(5.5)$$

和由它们导出的条件. 应该指出多于一个生成元的自由阿贝尔群不是自由群,因为非平凡关系 $xyx^{-1}y^{-1}=e$ 适用于阿贝尔群而不适用于自由群.

§ 32. **定义关系.** 设G是n个元素所生成的群，比如说

$$G=\mathrm{gp}\{g_1,g_2,\cdots,g_n\}.$$

那么G的每一元素是形为 $g_a^\alpha g_b^\beta\cdots g_r^\rho$的积. 除非$G$是自由群,否则总存在非平凡关系,例如

$$g_a^\alpha g_b^\beta\cdots=g_c^\gamma g_d^\delta\cdots,$$

或者用更简明的记号

$$r(g_1,g_2,\cdots,g_n)=1, \tag{5.6}$$

此处左边代表

$$(g_a^\alpha g_b^\beta\cdots)(g_c^\gamma g_d^\delta\cdots)^{-1}.$$

为了更详细地分析这情况,我们考虑n个符号上的自由群F,并定义F到G上的映射

$$\theta: F\to G,$$

其中θ用下面的规律定义

$$w(x_1,x_2,\cdots,x_n)\theta=w(g_1,g_2\cdots g_n), \tag{5.7}$$

即x的任一乘积在θ下的象是对应的g的积；特别

$$e\theta=1.$$

要指出的重要事实是θ是同态. 因而假如w_1与w_2是F的任意元素，那么

$$(w_1w_2)\theta=(w_1\theta)(w_2\theta). \tag{5.8}$$

这是由于(w_1w_2)定义为用w_1与w_2并列然后利用规律(5.2)与(5.5)进行简化而得出的简化字. 但是这些规律适用于任一群，作用在x_i上的运算对g_i也有效,而这正是(5.8)所指的. 考虑到θ是同态这事实,我们可以更简单地用

$$x_i\theta=g_i\quad(i=1,2,\cdots,n) \tag{5.9}$$

来指明这个同态. 从而由重复应用(5.9)而得到(5.7). 设R是θ的核,即R由所有F的那些字$r(x_1,x_2,\cdots,x_n)$组成，它们被θ映射到G中的关系(5.6)的左边. 我们记得由第一同构定理，

$$G\cong F/R. \tag{5.10}$$

总结我们的结果，能够述说下面的定理.

定理 17 设F是$x_1,x_2,\cdots,x_n$上的自由群. 那么n个元素$g_1,g_2,\cdots,g_n$所生成的任一群G是F关于映射$x_i\theta=g_i(i=1,2,\cdots,n)$的同态象. θ的核由所有那些F的字组成，它们在θ的作用下变成G中的关系.

出现在(5.10)的右边的这一对群F，R称为形成G的一个表现. 一个群可以具有许多这样的表现. 反之，选择F的某一正规子群R，定义G为F/R. 那么G具有生成元$g_i=x_iR(i=1,2,\cdots,n)$以及关系$r(g_1,g_2,\cdots,g_n)=1$，此处$r(x_1,x_i,\cdots,x_n)$遍历R. 因为$q(g_1,g_2,\cdots,g_n)=1$是G的关系当且仅当$q(x_1,x_2,\cdots,x_n)R=R$，即$q(x_1,x_2,\cdots,x_n)\in R$. 因而$R$的元素是与$G$的生成元所满足的关系一一对应. 由于这理由，我们将称R为G的**关系群**.

§ 33. 群的定义. 我们现在详细讨论G被n个生成元$g_1,g_2,\cdots g_n$和m个关系

$$\rho_k(g_1,g_2,\cdots,g_n)=1 \quad (k=1,2,\cdots,m) \tag{5.11}$$

所定义究竟意味着什么. 假如$\sigma(g_1,g_2,\cdots,g_n)=1$及$\tau(g_1,g_2\cdots,g_n)=1$是$G$的关系，那么下面这些式子也是$G$的关系

$$\sigma(g_1,g_2,\cdots,g_n)\tau(g_1,g_2,\cdots,g_n)=1,$$
$$\{\sigma(g_1,g_2,\cdots,g_n)\}^{-1}=1,$$

及

$$g^{-1}\{\sigma(g_1,g_2,\cdots,g_n)\}g=1,$$

此处g是G的任一元素. 任一关系，比如说

$$\rho(g_1,g_2,\cdots,g_n)=1, \tag{5.12}$$

它从所给的关系(5.11)应用任意有限次上面的运算而导出，则称之为(5.11)的**导出关系**.

利用$x_1,x_2,\cdots,x_n$上的自由群F，我们将字$r=\rho(x_1,x_2,\cdots,x_n)$与关系(5.12)相联系. 不失普遍性，我们可以假定这

是一个简化字，因此它是 F 的一个元素．例如，我们将不承认关系

$$g_1g_2g_2^{-2}g_1g_2^{-1}=1,$$

而是用

$$g_1g_2^{-1}g_1g_2^{-1}=1$$

来代替它．关系(5.11)对应于字

$$r_k=\rho_k(x_1,x_2,\cdots,x_n)(k=1,2,\cdots,m). \quad (5.13)$$

这些关系以及所有它们的导出关系构成 F 中含有 $r_1,r_2,\cdots,r_m$ 的最小正规子群 R_0，它表示成

$$R_0=\{r_1,r_2,\cdots,r_m\}^F,$$

称为 $r_1,r_2,\cdots,r_m$ 的**正规闭包**．它恰好就是由所有元素 $w^{-1}r_kw$ 所生成的 F 的子群，此处 r_k 取遍 $r_1,r_2,\cdots,r_m$，而 w 是 F 的任意元素．注意 R_0 由(5.11)及 F 完全决定．根据定理 17，G 与 F/R 同构，此处 R 是 G 的关系群．因为 R 是所有使得 $r(g_1,g_2,\cdots,g_n)=1$ 是 G 的关系的字 $r(x_1,x_2,\cdots,x_n)$的集，于是R_0 的每一元素属于 R，即

$$R_0\leqslant R. \quad (5.14)$$

假如

$$R_0=R, \quad (5.15)$$

我们将说 G 由生成元 $g_1,g_2,\cdots,g_n$ 及关系(5.11)所定义，或者更简短地说，(5.11)是 G 的一组**定义关系**．表达得更随便些，只要一开始就假设 G 为 n 个元素所生成，那么条件(5.15)说明所给条件(5.11)以及它们的导出关系包含所有可能的关于 G 的构造的信息．顺便指出，我们并不规定生成元或者关系是不多余的．在大多数实际情况中，少数关系就足够定义一个群，然而除非(5.11)是空的，正规闭包 R_0 一般是无限群，因此通常难以计算，而描述 G可能不得不依靠间接方法．

接着我们必须考虑下面的存在性问题：给出一组关系式

(5.11)，是否存在 n 个生成元上的群 G，对于它(5.11)是一组定义关系？一个简单的构造表明这问题的答案是肯定的．从(5.11)出发，我们构造正规闭包 R_0，并令

$$G_0=F/R_0 \tag{5.16}$$

这群由 n 个陪集

$$g_i^0=x_iR_0 \quad (i=1,2,\cdots,n)$$

生成，它们满足所有的关系(5.11)．事实上，

$$\rho_k(g_1^0,g_2^0,\cdots,g_n^0)=\rho_k(x_1,x_2,\cdots,x_n)R_0=r_kR_0=R_0,$$

因为 $r_k\in R_0$．现在假设 R 是 G_0 的关系群，它的定义在§32 的末尾，那么

$$G_0\cong F/R.$$

假如 $r(x_1,x_2,\cdots,x_n)$ 是 R 的任一元素，当 x_i 被 $g_i^0(i=1,\cdots,n)$ 代替时，它成为 G_0 的一个关系．因而我们有

$$r(g_1^0,g_2^0,\cdots,g_n^0)=r(x_1,x_2,\cdots,x_n)R_0=R_0,$$

从而 $r\in R_0$．这意味着 $R\leqslant R_0$，它与(5.14)一起可得出(5.15)．因而(5.11)是一组 G_0 的定义关系．当 $R_0=F$ 时，只有平凡群满足(5.11)．

我们构造的群 G_0 是满足(5.11)的"最大"或"最自由"的群．这一点用下面的定理可以说得更准确．

定理 18 设 $G=\mathrm{gp}\{g_1,g_2,\cdots,g_n\}$ 是具有下面定义关系的群

$$\rho_k(g_1,g_2,\cdots,g_n)=1_G \quad (k=1,2,\cdots,m). \tag{5.17}$$

假设 $H=\mathrm{gp}\{h_1,h_2,\cdots,h_n\}$ 满足同样的关系，即

$$\rho_k(h_1,h_2,\cdots,h_n)=1_H \quad (k=1,2,\cdots,m)$$

以及其他可能的不是它们的导出关系的关系，那么，借助于映射 ε：$G\to H$，ε 定义为

$$g_i\varepsilon=h_i \quad (i=1,2,\cdots,m),$$

H 是 G 的同态象．

证明 因为 G 与 H 具有 n 个生成元，存在满同态

$$\theta: F \to G, \quad \eta: F \to H,$$

具有核 R 与 S，它们分别是 G 与 H 的关系群. 利用(5.15)式，我们有

$$R = R_0,$$

因为(5.17)是一组 G 的定义关系. 关于 H 的假设等于说

$$S \geqslant R_0 (= R). \tag{5.18}$$

我们于是转到去构造一个映射 ε,

$$\varepsilon: G \to H$$

(见图 2)，设 $u = w(g_1, g_2, \cdots, g_n)$ 是 G 的任一元素，因为 θ 是满同态，

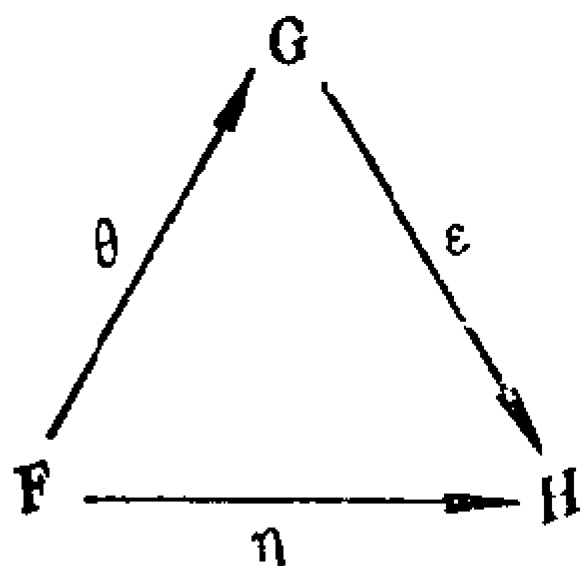


图 2

于是存在 F 的元素 z，例如 $z = w(x_1, x_2, \cdots, x_n)$（见(5.7)），使得

$$z\theta = u. \tag{5.19}$$

当 u 给定时，(5.19)的最一般解是 zr，此处 r 是 R 的任意元素. 因为 $z\theta = z'\theta$ 当且仅当 $z^{-1}z'$ 属于 R. 我们接着断定：假如 z 满足(5.19)，方程

$$u\varepsilon = z\eta \tag{5.20}$$

决定一个从 G 到 H 上意义明确的映射 ε，即我们必须验证，假如我们用 zr 代 z，(5.20)右边保持不变. 但是

$$(zr)\eta = (z\eta)(r\eta) = z\eta,$$

因为由(5.18)，$r \in S$，因而 $r\eta = 1_H$. 容易验证

$$(u_1\varepsilon)(u_2\varepsilon) = (u_1u_2)\varepsilon,$$

所以 ε 的确是同态. 特别，当 $u=g_i$ 时，我们可以令 $z_i=x_i$，于是得出

$$g_i\varepsilon=x_i\eta=h_i \quad (i=1,2,\cdots,n).$$

显然，它完全决定了 ε，这说明 ε 是满同态.

在我们以前(§12)非正式地研究过的群中完成这个论证是有益的. 于是设 $G=\mathrm{gp}\{a,c\}$ 是由如(2.27)的关系

$$a^3=c^2=(ac)^2=1 \tag{5.21}$$

所定义. 我们利用在生成元 x 与 y 上的自由群 F 将元素

$$r_1=x^3, \quad r_2=y^2, \quad r_3=(xy)^2$$

与(5.21)中所给的三个关系式相联系，设

$$R_0=\{r_1,r_2,r_3\}^F$$

及 $G_0=F/R_0$. G_0 的元素是陪集 wR_0，此处 $w\in F$，容易看出每一陪集等于

$$R_0, xR_0, x^2R_0, yR_0, yxR_0, yx^2R_0 \tag{5.22}$$

中的一个. 例如，$xyR_0=yx^2R_0$，因为 $xy=yx^2r$，此处

$$r=r_1^{-1}(xr_2^{-1}x^{-1})r_3$$

是 R_0 的元素. 目前我们还不能断定(5.22)中的六个陪集是不同的；因为可能有(5.21)的隐藏的导出关系使得某些陪集相等. 可是，$|G_0|\leqslant 6$，而我们知道假如 H 是任意一个两个生成元的满足(5.21)的群，那么，H 是 G 的同态象，因而 $|H|\leqslant|G_0|$，现在碰巧 $H=S_3$ 满足这些要求. 因为 S_3 由下列元素生成：

$$\alpha=(123), \quad \gamma=(12)$$

以及

$$\alpha^3=\gamma^2=(\alpha\gamma)^2=\iota.$$

既然 $|S_3|=6$，我们推断 $|G_0|=6$，因此 $G_0\cong S_3$.

作为这些思想的进一步应用，我们说明使 G 阿贝尔化的方法，即从 G 转变到 G/G'，它是 G 的最大阿贝尔同态象，这等于在原来的关系之外加上关系，

$$g_i^{-1}g_j^{-1}g_ig_j=1\ (i<j).$$

G/G' 的结构于是可以用第四章的方法直接找到，

例 当 G 是四元数群

$$a^4=1,a^2=b^2,ba=a^3b \tag{5.17}$$

时，找出 G/G'的构造.

阿贝尔群 G/G' 由$\bar{a}=aG'$与$\bar{b}=bG'$所生成. 在加法记号中，$\bar{a},\bar{b}$ 满足从(5.17) 导出的关系

$$4\bar{a}=0,2\bar{a}=2\bar{b},\bar{b}+\bar{a}=3\bar{a}+\bar{b}.$$

这些方程简化为

$$2\bar{a}=2\bar{b}=0.$$

对应的关系矩阵已经是对角形式，从而我们推断

$$G/G'\cong C_2\oplus C_2.$$

假如在$x_1,x_2,\cdots,x_n$上的自由群F用这种方法转变成阿贝尔群. 我们得出$F/F'=\langle\bar{x}_1,\bar{x}_2,\cdots,\bar{x}_n\rangle$(见§26)，此处$\bar{x}_i=x_iF'$. 因而 F/F' 是在 n 个生成元上的自由阿贝尔群.顺便指出从这论述得出，在不同个数生成元上的自由群不能是同构的. 因为设 F_m 与F_n 分别是 m 和 n 个生成元上的自由群，又假设它们是同构的. 那么 F_m/F_m' 与 F_n/F_n' 也会是同构的，但是它们分别是 m 与n 个生成元的自由阿贝尔群. 而我们知道它们不可能同构，除非 $m=n$(见 26). 最后我们不加证明地提出，每一个自由群的子群都是自由群这个重要但是困难的定理*.

习 题

(1) 证明自由群的导出群由那些字组成，其中每一个生成元的指数和等于零.(例如，$x_1x_2^{-1}x_1^{-2}x_2x_1$.)

---

* 见 Marshall Hall,Jr,*The Theory of groups*,p.96.(有中译本《群论》，裘光明译.科学出版社，1981.)

(2) 当 G 由(i) $a^6=b^2=(ab)^2=1$,(ii)$a^6=1,b^2=(ab)^2=a^3$ 给定时，决定 G/G' 的构造.

(3) 证明假如 G 由 a,b 生成：a,b 服从关系 $a^{-1}ba=b^2,b^{-1}ab=a^2$，那么 $G=\{1\}$.

第六章　子　群　列

§ 34.子群列. 在数学上研究复杂对象时通常将它们分解成较简单的"不可约"成分，比如整数分解成素数，多项式分解成不可约因子，等等．为了使这种分解有意义，分解必须是唯一的．这一点与所研究对象的内在性质相符.

在群G的情况中，这方法在于用适当的附加的性质考查某些下降或上升的子群序列

$$A_1 \geqslant A_2 \geqslant \cdots \quad 或 \quad B_1 \leqslant B_2 \leqslant \cdots \tag{6.1}$$

我们希望每一子群列能阐明G的一些构造，但结果是，没有一个能够完全刻画G．序列(6.1)称为*子群列*.（这里借用序列一词需要得到分析学家的谅解.）

§ 35. 约当-霍尔德(Jordan-Hölder)定理. 我们记得,假如一个群的阶大于1,又没有非平凡正规子群,这个群就称为单群（§ 19)．对于任意一个群，下面的定义描写了一类重要的正规子群.

定义 5　*正规子群$A(\neq G)$称为G的***极大正规子群***,假如不存在与G,A不同的正规子群H,使得*

$$G \triangleright H \triangleright A.$$

由命题10 (§ 22),这等于说G/A没有真正规子群．因而上面的定义可以改写为

判别准则　*正规子群$A(\neq G)$是G的极大正规子群，当且仅当G/A是单群.*

一个群可以有几个构造和阶彼此不同的极大正规子群．假如G/A是素数阶，那么A是极大正规子群．还有,假如G是单群，那么$\{1\}$是唯一的极大正规子群.

为了简化讨论，我们在本节余下部分限于讨论有限群．得出

的结果也适用某些类型的无限群(例如见 A．G．Kurosh.*Theory of groups*. 1,110—116)，但是我们想到的应用只牵涉有限群．假如 G 不是单群，设 A_1 是它的某一个极大正规子群；其次设 A_2 是 A_1 的极大正规子群，A_3 是 A_2 的极大正规子群等等．因为我们所定义的这些群的阶是严格下降的，最后我们一定会到达单位元群。因而导致下面的定义：

定义 6　*群 $G(=A_0)$ 的子群序列*

$$A_1, A_2, \cdots, A_r \tag{6.2}$$

*称为 G 的***合成列**．*假如*

(i) $G \triangleright A_1 \triangleright A_2 \triangleright \cdots \triangleright A_r \triangleright \{1\}$　　(6.3)

且

(ii) $G/A_1, A_1/A_2, \cdots, A_{r-1}/A_r, A_r$　　(6.4)

是单群．

必须清楚地理解当 A_i 在 A_{i-1} 中是正规的，又的确是极大正规子群时，A_i 不需要在(6.3)序列中 A_i 前面任一另外的群中是正规的．特别，在(6.2)的那些群中，只有 A_1 必须是 G 的正规子群．(6.4)中所列出的商群称为**合成商群**或**合成因子**．

因为极大正规子群一般不是唯一的，一个群可以有不止一个的合成列．可是，下面的基本定理肯定合成因子(直到重排和同构)是唯一的．因此合成因子组构成群的固有性质．我们将只对有限群证明这结论．

定理 19(约当-霍尔德)　*在有限群的任意两个合成列中，合成因子，除它们的次序外，是成对同构的．*

证明　让我们详细地分析这说法．设

$$G(=A_0) \triangleright A_1 \triangleright A_2 \triangleright \cdots \triangleright A_r \triangleright \{1\} \tag{I}$$

及

$$G(=B_0) \triangleright B_1 \triangleright B_2 \triangleright \cdots \triangleright B_s \triangleright \{1\} \tag{II}$$

是 G 的两个合成列．假如合成因子

$$G/A_1,\ A_1/A_2,\cdots,A_{r-1}/A_r,A_r \tag{I}'$$

及

$$G/B_1,B_1/B_2,\cdots,B_{s-1}/B_s,B_s \tag{II}'$$

除重新排列外，是成对同构的，我们将写为(I)～(II). 显然，这在所有的合成列中建立了一个等价关系，我们的目的在于证明所有合成列在这个意义下是等价的. 注意，特别，(I)～(II)意味着 $r=s$.

当 G 是单群，唯一可能的合成列是 $G\triangleright\{1\}$. 在这情况，列(I)与(II)肯定是相同的，而我们有 $r=s=0$. 因而定理显而易见适用于所有单群，而特别适用于所有阶小于 4 的群.

我们将对于 $|G|$ 用归纳法进行讨论，而且略去单群的情形，即我们今后假定 $r\geqslant 1$ 及 $s\geqslant 1$. 必须区分两种情况

(i) $A_1=B_1$. 略去(I)与(II)中的第一项，我们得到两个 A_1 的合成列，即

$$A_1\triangleright A_2\triangleright\cdots\triangleright A_r\triangleright\{1\}$$

及

$$A_1\triangleright B_2\triangleright\cdots\triangleright B_s\triangleright\{1\}.$$

因为 $|A_1|<|G|$，归纳假设意味合成因子

$$A_1/A_2,A_2/A_3,\cdots,A_r$$

及

$$A_1/B_2,B_2/B_3,\cdots,B_s$$

是成对同构的. 因为(I)′与(II)′的第一项现在是相同的，所以我们有(I)～(II). 于是在这情况下定理已证明.

(ii) $A_1\neq B_1$. 因为 $A_1\triangleleft G$ 及 $B_1\triangleleft G$，群(见§ 15)

$$C=A_1B_1(=B_1A_1)$$

是在 G 中正规的，且包含 A_1 与 B_1 作为子群，特别

$$G\geqslant C\geqslant A_1.$$

但是 A_1 是 G 的极大正规子群，因而或者 $C=G$ 或者 $C=A_1$. 后一

个可能性必须放弃,因为,既然 $B_1<C$,这意味 $G>A_1>B_1$,这与 B_1 是极大正规子群的事实是不相容的. 因而

$$G=A_1B_1.$$

设 $D=A_1\cap B_1$. 应用定理 10(§ **22**)我们得出

$$G/A_1\cong B_1/D,\ G/B_1\cong A_1/D. \tag{6.5}$$

根据 G/A_1 与 G/B_1 的构造是单群,因而 B_1/D 及 A_1/D 也是单群,即 D 是 A_1 与 B_1 二者的最大正规子群. 设

$$D\triangleright D_1\triangleright\cdots\triangleright D_t\triangleright\{1\}$$

是 D 的任一合成列. 我们因而能构造两个 G 的合成列,即

$$G\triangleright A_1\triangleright D\triangleright D_1\triangleright\cdots\triangleright D_t\triangleright\{1\} \tag{III}$$

及

$$G\triangleright B_1\triangleright D\triangleright D_1\triangleright\cdots\triangleright D_t\triangleright\{1\}. \tag{IV}$$

事实上,所有合成因子

$$G/A_1, A_1/D, \vdots\ D/D_1,\cdots,D_t \tag{III$'$}$$

及

$$G/B_1, B_1/D, \vdots\ D/D_1,\cdots,D_t \tag{IV$'$}$$

象刚才所看到的那样,都是单群.垂直线右边的合成因子对于(III)′与(IV)′是相同的,而垂直线左边的合成因子当交叉配对时是成对同构的,因而(III)~(IV). 因为(I)与(III)的头两项相同,这是我们在(i)中讨论过的情况,因而(I)~(III).相似地,(II)~(IV). 因而我们断定(I)~(II). 这就完成了证明.

我们用两个例子说明这定理,它们都相当简单. 因为我们还没有碰见过阶为合数的单群(见 § **41**).

(1) 设 G 是 6 阶(§ **14**)的非阿贝尔群,它能用下面的关系定义:

$$a^3=b^2=(ab)^2=1.$$

子群 $A=\mathrm{gp}\{a\}$ 是 3 阶群,在 G 中的指数是 2. 因而 $A\triangleleft G$(§ **19**

(iv)),及

$$G \rhd A \rhd \{1\}$$

是合成列，因为因子

$$G/A \cong C_2 \text{ 及 } A \cong C_3 \tag{6.6}$$

是素数阶的因而是单群.

(2) 设 $G = \mathrm{gp}\{s\}$是 6 阶循环群. 那么 $A_2 = \mathrm{gp}\{s^2\}$ 是 3 阶子群. 又因为阿贝尔群的所有子群是正规的，我们有合成列

$$G \rhd A_2 \rhd \{1\}$$

见有合成因子

$$G/A_2 \cong C_2 \text{ 与 } A_2 \cong C_3. \tag{6.7}$$

或者，我们能从 2 阶子群 $A_3 = \mathrm{gp}\{s^3\}$开始，构成合成列

$$G \rhd A_3 \rhd \{1\},$$

它的因子

$$G/A_3 \cong C_3 \text{ 及 } A_3 \cong C_2$$

与(6.7)相同，但是次序相反. 我们看到，虽然(1)与(2)中的群G不是同构的，但在(1)与(2)中出现的合成因子是相同的. 在两种情况中合成因子都是素数阶. 这个性质是很重要一类群的特点. 我们将在下节研究.

§ 36. 可解群.

定义 7 有限群称为**可解的**，假如它的所有合成因子是素数阶.

下面的命题常用来决定给定的群是否是可解的.

命题 15 假如有限群G包含正规子群H，使得H与G/H是可解的，则G是可解的.

证明 假如这些条件满足，我们有合成列

$$H \rhd H_1 \rhd \cdots \rhd H_r \rhd \{1\} \tag{6.8}$$

及

$$G/H \rhd G_1/H \rhd \cdots \rhd G_s/H \rhd H. \tag{6.9}$$

(应该记得 G/H 的任一子群可以写成 A/H，以及 H 是 G/H 的单位元素.)由假设，(6.8)与(6.9)的合成因子是素数阶的，特别，G_s/H 有素数阶. 因为由定理9（§ **22**）

$$\frac{G_{i-1}/H}{G_i/H}\cong G_{i-1}/G_i \quad (G_0=G),$$

我们推断

$$G\triangleright G_1\triangleright G_2\triangleright\cdots\triangleright G_s\triangleright H\triangleright H_1\triangleright\cdots\triangleright H_r\triangleright\{1\}$$

是 G 的合成列，其中每一合成因子是素数阶. 因而 G 是可解的. 这个结论的用处由下面的应用来说明.

命题 16 所有有限阿贝尔群是可解的.

证明 设 A 是有限阿贝尔群. 假如 $|A|=p$，此处 p 是素数，那么合成列

$$A\triangleright\{1\}$$

指出 A 的可解性. 于是我们关于 $|A|$ 应用归纳法，而且假设 A 的阶是合数. 那么 A 具有真子群 H（第二章，习题4），H 在 A 中必然是正规的. 因为 H 与 A/H 是阶较 $|A|$ 小的阿贝尔群，归纳假设意味 H 及 A/H 是可解的，因而由命题15 A 是可解的.

命题 17 所有有限 p-群是可解的.

证明 设 P 是有限群使得 $|P|=p^n$，此处 p 是素数. 当 $n=1$，群肯定是可解的. 所以我们关于 n 用归纳法. 由定理7（§ **18**），P 的中心 Z 是非平凡的，于是必然 $Z\triangleleft P$. 现在，Z 是可解的，因为它是阿贝尔群；而 P/Z 是 P-群，它的阶小于 p^n，因而由归纳法 P/Z 是可解的. 于是由命题15，P 是可解的.

最后，我们提出可解群的一个刻画. 它似乎比原来的定义需要的条件更宽.

命题 18 有限群 G 是可解的当且仅当具有子群 $B_1,B_2,\cdots,B_s$ 使得

$$G\triangleright B_1\triangleright B_2\triangleright\cdots\triangleright B_s\triangleright\{1\}\quad (G=B_0,\{1\}=B_{s+1}),\quad(6.10)$$

而

$$每一B_{i-1}/B_i 是阿贝尔群(i=1,2,\cdots,s+1). \qquad (6.11)$$

证明　假如G是可解的．那么由定义 7 存在一个列(6.10)，其中B_{i-1}/B_i是素数阶的，因此是阿贝尔群．反之，假定(6.10)与(6.11)成立，我们可以假设在(6.10)中没有多余的项，所以每一群是它的前项的真子群．我们用关于$|G|$的归纳法进行讨论．略去(6.10)的首项，我们对B_1得出一列，由归纳法，这意味B_1是可解的．在(6.11)中使$i=1$，我们看到G/B_1是阿贝尔群因而是可解的．因而由命题 15，G是可解的．

§ 37．导出列．　G的导出群G'以及它的某些性质已在 § 23 中介绍过．我们记起（定理 11）G'是最小的具有阿贝尔商群的正规子群．形成导出群的过程可以重复．因而我们构成序列

$$G=(G_0),G',G''=(G')',\cdots,G^i=(G^{i-1})',\cdots.$$

因为$G^{(i)}\leqslant G^{(i-1)}$，我们能够写成

$$G\geqslant G'\geqslant G''\geqslant\cdots\geqslant G^{(i)}\geqslant\cdots. \qquad (6.12)$$

这称为群G的**导出列**．(6.12)中每一群不仅在它的前项中是正规的，而且是前一项的特征子群(见第三章习题 14)，因而是G本身的正规子群．这导出列可能终止于某一项，即对某一i，$G^{(i+1)}=G^{(i)}$．当然，当G是有限时，这必然会出现．可是我们最感兴趣的情况是(6.12)终止于单位元群，因为这还给出可解群的另一种描写．

定理 20　有限群G是可解的当且仅当它的导出列终止于单位元群．即$G^{(s)}=\{1\}$，对于某一非负整数s．

证明　(i) 假设$G^{(s)}=\{1\}$，因此导出列是

$$G>G'>G''>\cdots>G^{(s-1)}>\{1\}. \qquad (6.13)$$

由定理 11，$G^{(i-1)}/G^{(i)}$是阿贝尔群．因而(6.13)是命题 18 中所考虑的那种类型的列，即G是可解的．

(ii) 假定G是可解的，因而具有一子群序列满足 (6.10) 与

(6.11). 我们断定

$$G^{(i)}\leqslant B_i \quad (i=1,2,\cdots). \tag{6.14}$$

因为 G/B_1是阿贝尔群,我们由定理 11 推导出 $G'\leqslant B_1$. 于是我们作归纳假设 $G^{(i-1)}\leqslant B_{i-1}$. 显然只要从导出群的定义, 即可知当 $K\leqslant L$ 时,$K'\leqslant L'$. 因而

$$G^{(i)}=(G^{(i-1)})'\leqslant B'_{i-1}\ .$$

因为 B_{i-1}/B_i 是阿贝尔群, 我们再一次用定理 11 来断定 $B'_{i-1}\leqslant B_i$,从而 $G^{(i)}\leqslant B_i$. 这证明了(6.14). 当 $i=s+1$ 时, 这结论成为

$$G^{(s+1)}\leqslant B_{s+1}=\{1\}.$$

因而导出列终止于单位元群.

§ 38. 幂零群. 在这节我们将介绍一类群. 它们的结构, 在最适于分析这一点上,仅次于阿贝尔群. 我们从推广 **§ 23** 上所定义的换位子概念开始. 对应 G 的任意子集 A , B ,我们可以构成子群

$$[A,B]=\mathrm{gp}\{[a,b]\mid a\in A,b\in B\}. \tag{6.15}$$

因为

$$[a,b]^{-1}=(a^{-1}b^{-1}ab)^{-1}=b^{-1}a^{-1}ba=[b,a],$$

那么

$$[A,B]=[B,A], \tag{6.16}$$

因为(6.15)中每一生成元的求逆并不改变所生成的群. 显然, 假如 $B\leqslant C$,那么$[A,B]\leqslant[A,C]$.

我们将任一群 G 与如下归纳定义的子群序列相联系:

$$\Gamma_1=G,\Gamma_2=[\Gamma_1,G]=G',\cdots,\Gamma_{k+1}=[\Gamma_k,G],\cdots. \tag{6.17}$$

我们将证明 $\Gamma_{k+1}\leqslant\Gamma_k(k=1,2,\cdots)$. 当 $k=1$ 这是显而易见的. 假设$\Gamma_k\leqslant\Gamma_{k-1}(k>1)$,我们推导出$\Gamma_{k+1}=[\Gamma_k,G]\leqslant[\Gamma_{k-1},G]=\Gamma_k$. 因而(6.17)事实上是一下降列

$$G=\Gamma_1\geqslant\Gamma_2\geqslant\cdots\geqslant\Gamma_k\geqslant\Gamma_{k+1}\geqslant\cdots. \tag{6.18}$$

每一 Γ_k 是 G 的特征子群, 即假如 α 是 G 的自同构, 那么 $\Gamma_k\alpha=\Gamma_k$

(见(3.50)). 因为,既然 $\alpha:G\to G$ 是同态, 我们有 $[a,b]\alpha=[a\alpha, b\alpha]$,因而 $[A,B]\alpha=[A\alpha,B\alpha]$. 现在 $G\alpha=G$ 及 $\Gamma_{k+1}\alpha=[\Gamma_k\alpha,G]$. 假如我们已经证明 $\Gamma_k\alpha=\Gamma_k$, 当 $k=1$ 这是显而易见的, 那么 $\Gamma_{k+1}\alpha=[\Gamma_k,G]=\Gamma_{k+1}$. 这证明

$$\Gamma_k\alpha=\Gamma_k(k=1,2,3\cdots).$$

从而 $\Gamma_k\lhd G(k=1,2,3,\cdots)$, 更有理由得出 $\Gamma_{k+1}\lhd\Gamma_k$. (6.18) 的一个不很明显的性质表示如下:

命题 19 商群 Γ_k/Γ_{k+1} 位于 G/Γ_{k+1} 的中心之内.

证明 设 $\nu:G\to G/\Gamma_{k+1}$ 是 G 到 G/Γ_{k+1} 上的自然映射, 即 $x\nu=x\Gamma_{k+1}=\bar{x}$, 此处 $x\in G$. ν 的核等于 Γ_{k+1}. Γ_k/Γ_{k+1} 的典型元素是 $\bar{u}=u\Gamma_{k+1}$, 此处 u 是 Γ_k 的任一元素. 我们必须证明对于所有的 x, $\bar{u}$ 与 $\bar{x}$ 交换. 即我们必须证明 $[\bar{u}, \bar{x}]=\bar{\iota}$, 此处 $\bar{\iota}(=\Gamma_{k+1})$ 是 G/Γ_{k+1} 的单位元素. 现在

$$[\bar{u},\bar{x}]=[u\nu,x\nu]=[u,x]\nu.$$

由 Γ_{k+1} 的定义, $[u,x]\in\Gamma_{k+1}$. 因而, $[u,x]\nu=\bar{\iota}$. 这证明了我们的断言.

下面, 我们将对任一群 G 定义一个上升列. 构造这上升列基于下引理.

引理 设 U 是 G 的特征子群, 又设 V/U 是 G/U 的中心, 那么 V 是 G 的特征子群.

证明 群 V 可以描写成与 G"模 U"交换的 G 的最大子群. 即

$$[V,G]\leqslant U.$$

事实上, 假如我们应用自然映射 $\mu:G\to G/U$, 它"杀掉" U, 这关系成为 $[V\mu,G\mu]=\{\bar{\iota}\}$, 此处 $\bar{\iota}$ 是 G/U 的单位元素. 这意味着 V/U $(=V\mu)$ 的每一元素与 $G/U=(G\mu)$ 的每一元素交换. 现在假设 α 是 G 的自同构, 那么 $[V\alpha,G]\leqslant U\alpha$. 根据假设, $U\alpha=U$, 因此 $[V\alpha,G]\leqslant U$. 因而, 由于 V 的最大性, $V\alpha\subset V$. 假如, 我们用自同构 α^{-1} 代替 α, 可类似地推导出 $V\alpha^{-1}\subset V$, 即 $V\subset V\alpha$. 因此 $V\alpha=$

V. 因而V是特征子群.

现在令 $Z_0=\{1\}$，又设 Z_1 是G的中心. 因为 Z_1是G的特征子群，我们从引理推导出存在特征子群 Z_2，使得 Z_2/Z_1是 G/Z_1的中心. 我们利用 Z_{j+1}/Z_j 是 G/Z_j 的中心，归纳地定义 Z_{j+1}. 因而我们构成一个特征子群的上升列：

$$\{1\}=Z_0\leqslant Z_1\leqslant\cdots\leqslant Z_j\leqslant\cdots. \qquad (6.19)$$

象我们所讲过的那样，对任一群 G，存在序列(6.18)，(6.19)，但是假如 $G=G'(=\Gamma_2)$，或者假如 $Z_1=\{1\}$，它们分别简化成一项. 我们对相反的情况最感兴趣，那时序列从群G伸展到单位元群$\{1\}$，因而具有最大长度.

定义 8 (i) 群G称为具有长度为r的**下中心群列**，假如

$$G=\Gamma_1>\Gamma_2>\cdots>\Gamma_k>\cdots>\Gamma_r>\Gamma_{r+1}=\{1\}, \qquad (6.20)$$

此处 $\Gamma_{k+1}=[\Gamma_k,G](k=1,2,\cdots,r)$.

(ii) 群G称为具有长度为s的**上中心群列**，假如

$$\{1\}=Z_0<Z_1<\cdots<Z_j<\cdots<Z_s=G, \qquad (6.21)$$

此处 Z_j/Z_{j-1} 是 G/Z_{j-1} 的中心$(j=1,2,\cdots,s)$.

象在引理中那样，Z_j 可以被刻画为G具有以下性质的最大子群

$$[Z_j,G]\leqslant Z_{j-1}. \qquad (6.22)$$

在两个中心群列的项之间存在某些值得注意的关系. 事实上，我们将发现，假如其中一列存在，另一列也一定存在，而且两个列具有相同的长度.

首先假设G具有长度为r的下中心列，因此(6.20)成立，接着对群G考虑列(6.19). 我们断定

$$\Gamma_{r+1-i}\leqslant Z_i \quad (i=0,1,\cdots,r). \qquad (6.23)$$

当 $i=0$ 时，显然这是正确的，因为已假设 $\Gamma_{r+1}=\{1\}=Z_0$. 作归纳假设如下：假如(6.23)对某一特殊的 i 成立，我们想要证明 $\Gamma_{r-i}\leqslant Z_{i+1}$. 因为 $\Gamma_{r+1-i}=[\Gamma_{r-i},G]$. 我们的假设是$[\Gamma_{r-i},G]\leqslant Z_i$. 由

(6.22)，Z_{i+1}是满足$[Z_{i+1},G]\leqslant Z_i$的最大子群。因此$\Gamma_{r-i}\leqslant Z_{i+1}$，因而对所有的$i$证明了(6.23)。特别，当$i=r$，我们得出$\Gamma_1=G\leqslant Z_r$。这意味着$Z_r=G$。因而(6.19)至多在$r$步之后终止于$G$，即$G$具有一个上中心群列，它的长度$s$满足

$$s\leqslant r. \tag{6.24}$$

其次，假定(6.21)对G成立，并对这个群考查列(6.18)。我们现在断定

$$\Gamma_i\leqslant Z_{s+1-i}\quad (i=1,2,\cdots,s+1). \tag{6.25}$$

当$i=1$时，这是正确的，因为我们已经假定$Z_s=G=\Gamma_1$。用归纳法进行证明，假设(6.25)对一特定i成立，而我们想证明$\Gamma_{i+1}\leqslant Z_{s-i}$。事实上，我们有$\Gamma_{i+1}=[\Gamma_i,G]\leqslant[Z_{s+1-i},G]\leqslant Z_{s-i}$，象所要求的那样。在(6.25)中，令$i=s+1$，我们断定$\Gamma_{s+1}\leqslant Z_0=\{1\}$，即$\Gamma_{s+1}=\{1\}$。因而(6.18)至多在$s+1$步以后终止于$\{1\}$，这证明了$G$具有下中心群列，它的长度$r$满足$r\leqslant s$. 与(6.24)一起，这证明了$s=r$。

前面的研究使我们最后能够确切定义本节开头提到的这类群。

定义 9 *群G称为**幂零群**，假如它具有下中心群列，或者，等价地，具有上中心群列. 这些列的公共长度称为G的幂零类数.*

例 1 假如A是阶大于1的阿贝尔群，那么上中心群列约化到

$$\{1\}=Z_0<Z_1=A,$$

因而阿贝尔群($\neq\{1\}$)的集与类数为1的幂零群的集一致.

例 2 *有限p-群是幂零群.* 假如P是有限p-群，那么由定理7(§18)，它的中心Z_1具有大于1的阶。现在P/Z_1也是p-群，因此它的中心Z_2/Z_1是非平凡的，即$Z_1<Z_2$。相似的，P/Z_2具有中心Z_3/Z_2，此处$Z_2<Z_3$。象这样继续下去，我们构成严格上升列

$$\{1\}=Z_0<Z_1<Z_2<Z_3<\cdots$$

因为 p 是有限的，这上升列一定会结束．比如说，这发生在 $Z_r=P$ 时．因而 P 具有上中心群列，因此是幂零群．从关于幂零群的许多结果中，我们选择一个有趣的事实，这个事实我们在本书末尾还要谈到．

命题20　假如 H 是幂零群 G 的真子群，那么 H 在 G 中的正规化子 $N(H)$ 严格大于 H．

证明　设 G 是类数为 r 的幂零群．显而易见，$\{1\}=Z_0\leqslant H$．在另一方面，因为 H 是真子群，$G=Z_r\not\leqslant H$．因而存在唯一的整数 k，使得 $0\leqslant k\leqslant r-1$ 而

$$Z_k\leqslant H,\ Z_{k+1}\not\leqslant H. \tag{6.26}$$

因而存在元素 u 使得 $u\in Z_{k+1}$ 及 $u\notin H$．只要证明 $u\in N(H)$，即

$$u^{-1}Hu=H \tag{6.27}$$

就够了．设 h_1 是 H 的任一元素，那么，由(6.22)及(6.26)，

$$[u,h_1]\in[Z_{k+1},G]\leqslant Z_k\leqslant H.$$

这意味着 $u^{-1}h_1^{-1}uh_1=h_2$，此处 $h_2\in H$．因而 $u^{-1}h_1^{-1}u\in H$．因为 h_1^{-1} 与 h_1 一起遍历 H，我们就证明了 $u^{-1}Hu\subset H$．当 u 用 u^{-1} 代替时，利用同样的论证我们断定 $uHu^{-1}\subset H$，即 $H\subset u^{-1}Hu$．这就证明了(6.27)．

习　题

(1) 求下列群的合成列：(i) 8 阶的二面体群 (§14，表 xi)．(ii) 四元数群(§14，表 xii)．决定每种情况中的合成因子．

(2) 证明可解群的每一子群和商群是可解的．

(3) 假如 x,y,z 是群的任意元素，证明：(i) $[xy,z]=[x,z]^y[y,z]$；(ii) $[x,yz]=[x,z][x,y]^z$，此处 $a^t=t^{-1}at$．

(4) 证明假如 G 是类数为 2 的幂零群，那么 G' 位于 G 的中心内，对这

样的群推导下列恒等式。

$$[xy,z]=[x,z][y,z],[x,yz]=[x,z][x,y].$$

(5) 证明幂零群的每一子群和商群是幂零群。

(6) 设 G 是类数为 3 的幂零群。证明，假如 $v\in G'$ 及 $x\in G$，那么 $x^v=cx$，此处 $c\in Z$，Z 是 G 的中心。推导 G' 是阿贝尔群。

(7) 证明假如 M 是幂零群 G 的极大子群，那么 $M\lhd G$ 及 $|G/M|=p$，此处 p 是素数。[极大子群是真子群，它不包含在任一其他真子群内。无限群不一定具有极大子群]。

(8) 设 $D(2^n)$是 2^{n+1} 阶二面体群(第二章习题 7)，用下面的关系式给出

$$a^{2^n}=b^2=(ab)^2=1.$$

证明假如 Z_1 是 $D(2^n)$的中心，那么 $D(2^n)/Z_1\cong D(2^{n-1})$。推导 $D(2^n)$ 是类数为 n 的幂零群。

第七章 置 换 群

§ **39.** S_n **的共轭类.** 在§**7**我们引入对称群族 $S_n(n=1,2,\cdots)$，描述了它们的某些基本性质.本章致力于这些群的更详细的研究，这些群及其子群在有限群论中起了基本的作用.

在本节中，我们考虑分解 S_n 到它的共轭类（见§**17**）的问题.为此，我们需要计算乘积 $\tau^{-1}\alpha\tau$ 的技巧，此处 α 与 τ 是 S_n 的任意元素. 利用（**1.43**）的符号，设

$$\alpha=\begin{pmatrix}1 & 2\cdots n\\ a_1 a_2 & \cdots a_n\end{pmatrix}. \tag{7.1}$$

这符号缩写为

$$\alpha=\begin{pmatrix}i\\ a_i\end{pmatrix}, \tag{7.2}$$

此处 $i=1,2,\cdots,n$. 为了简化符号，我们设

$$\tau=\begin{pmatrix}12 & \cdots & n\\ 1'2' & \cdots & n'\end{pmatrix}=\begin{pmatrix}i\\ i'\end{pmatrix}, \tag{7.3}$$

此处 $1'2'\cdots n'$ 是 $1\ 2\ldots n$ 对应于 τ 的重新排列. 象我们在§**7**所说过的那样，关于 τ 的说明可以用非标准形式表达，其效果是同样的. 特别，我们可以写成

$$\tau=\begin{pmatrix}a_i\\ a_i'\end{pmatrix}, \tag{7.4}$$

此处（**7.4**）的第一行与（**7.1**）的第二行是相同的. 我们于是有

$$\tau^{-1}\alpha\tau=\begin{pmatrix}i'\\ i\end{pmatrix}\begin{pmatrix}i\\ a_i\end{pmatrix}\begin{pmatrix}a_i\\ a_i'\end{pmatrix}=\begin{pmatrix}i'\\ a_i'\end{pmatrix}.$$

这结果可以描述如下：为了得出 $\tau^{-1}\alpha\tau$，可用 τ 作用在 α 的表示式的每一符号上，即作用在（7.1）的两行上，因而

$$\tau^{-1}\alpha\tau=\begin{pmatrix} i\tau \\ a_i\tau \end{pmatrix}. \tag{7.5}$$

例 设 $n=4$ 及

$$\alpha=\begin{pmatrix} 1\,2\,3\,4 \\ 2\,4\,1\,3 \end{pmatrix},\quad \tau=\begin{pmatrix} 1\,2\,3\,4 \\ 1\,4\,2\,3 \end{pmatrix}.$$

用 τ 作用在 α 的每一符号上我们得出

$$\tau^{-1}\alpha\tau=\begin{pmatrix} 1\,4\,2\,3 \\ 4\,3\,1\,2 \end{pmatrix}=\begin{pmatrix} 1\,2\,3\,4 \\ 4\,1\,2\,3 \end{pmatrix}.$$

其次，应用这个方法到 m 次轮换，比如说

$$\gamma=(a_1a_2\ldots a_m)=\begin{pmatrix} a_1a_2\cdots a_{m-1}a_m \\ a_2a_3\cdots a_m\ a_1 \end{pmatrix}.$$

因而由 (7.5)，

$$\tau^{-1}\gamma\tau=\begin{pmatrix} a_1'a_2'\cdots a'_{m-1}a'_m \\ a_2'a_3'\cdots a'_m a_1' \end{pmatrix}=(a_1'\ a_2'\ \cdots a_m'),$$

或者更简单地

$$\tau^{-1}\gamma\tau=(a_1\tau\ \ a_2\tau\ \cdots\ a_m\tau). \tag{7.6}$$

我们已经知道（§7，定理 2）每一置换 α 能用本质上唯一的方式表成不相交轮换的积，因而

$$\alpha=\gamma_1\gamma_2\cdots\gamma_r \tag{7.7}$$

此处 $\gamma_1,\gamma_2,\cdots,\gamma_r$ 是不相交的轮换，分别含有

$$m_1,m_2,\cdots,m_r \tag{7.8}$$

个对象．对于目前的讨论，保留长度为 1 的轮换使得所有 n 个对象都在乘积 (7.7) 中列出是方便的． (7.8) 中的整数称为 α 的**轮换类型**．将 (7.8) 中的数按数值增加的次序排列是方便的．因而所有可能的 S_n 的轮换类型与 (7.8) 中的满足下列条件的这组整数一一对应：

$$1\leqslant m_1\leqslant m_2\leqslant\cdots\leqslant m_r$$

及

$$m_1+m_2+\cdots+m_r=n, \tag{7.9}$$

γ是任意的. 或者，假如α包含e_1个1次轮换，e_2个2次轮换，$\cdots$，e_n个n次轮换，则α的轮换类型可以用下列非负整数描写

$$e_1, e_2, \cdots, e_n,$$

它们满足

$$e_1+2e_2+\cdots+ne_n=n. \tag{7.10}$$

下面的结果将轮换类型与S_n的共轭类联系.

命题 21 两个置换在S_n中共轭当且仅当它们具有相同的轮换类型.

证明 设α分解成不相交轮换，因而

$$\alpha=\gamma_1\gamma_2\cdots\gamma_r=(x_1x_2\cdots)(y_1y_2\cdots)\cdots(w_1w_2\cdots),$$

此处γ_i是m_i次，$m_1+m_2+\cdots+m_r=n$.

假如τ是任意象(7.3)中所指出的那样的置换，那么

$$\begin{aligned}\beta=\tau^{-1}\alpha\tau&=(\tau^{-1}\gamma_1\tau)(\tau^{-1}\gamma_2\tau)\cdots(\tau^{-1}\gamma_r\tau)\\&=(x_1'\,x_2'\cdots)(y_1'\,y_2'\cdots)\cdots(w_1'\,w_2'\cdots)\\&=\gamma_1'\gamma_2'\cdots\gamma_r'.\end{aligned}$$

此处$\gamma_1'\gamma_2'\cdots\gamma_r'$是不相交轮换，因为$\tau$是一一映射. 因而$\beta$具有与$\alpha$相同的轮换类型.

反之，假如α与β象上面那样，具有相同的轮换类型，那么置换

$$\tau=\begin{pmatrix}x_1x_2\cdots y_1\,y_2\cdots & w_1w_2\cdots\\ x_1'x_2'\cdots y_1'\,y_2'\cdots & w_1'\,w_2'\cdots\end{pmatrix}$$

具有性质$\tau^{-1}\alpha\tau=\beta$，因而$\alpha$与$\beta$共轭.

因而S_n中存在的共轭类与S_n中可能有的轮换类型同样多，换句话说，S_n中的共轭类个数k等于将n分成正加数的划分(7.9)的个数，或者等于将n分成非负加数的划分(7.10)的个数. 当用后一种说法时，常将划分表示为

$$1^{e_1}2^{e_2}\cdots n^{e_n},\tag{7.11}$$

频率为零的部分在具体情况下常被省略，例如

$$1^3 3\, 4^2$$

是 14 的划分1+1+1+3+4+4. 不幸，没有简单的公式能够将类的个数 k 表示成 n 的函数. 下面的表对开头几个 n 的值给出了 k.

n	1	2	3	4	5	6	7	8
k	1	2	3	5	7	11	15	22

[表(xiii)]

例如，当 $n=5$，划分 (7.11) 是

$$1^5, 1^3 2, 1^2 3, 12^2, 14, 23, 5.$$

在另一方面，不难说出某一特殊的 S_n 的共轭类中有多少元素.

命题 22 (哥西 Cauchy) *假设 α 具有对应划分 $1^{e_1}2^{e_2}\cdots n^{e_n}$ 的轮换类型，那么在 S_n 中与 α 共轭的置换个数等于*

$$h_\alpha=\frac{n!}{1^{e_1}e_1!2^{e_2}e_2!\cdots n^{e_n}e_n!}.\tag{7.12}$$

证明 轮换类型 α 可以用下图表示

$$\underbrace{(\cdot)\ (\cdot)\cdots\ (\cdot)}_{e_1}\ \underbrace{(\cdot\cdot)(\cdot\cdot)\cdots(\cdot\cdot)}_{e_2}\cdots,\tag{7.13}$$

它对应划分 (7.11).

在 (7.13)中恰好有 n 个空位，将 n 个对象用任意方式填进去，我们就得出 S_n 的一个元素. 在每一情况下我们都得到一与 α 有相同轮换类型的置换. 共有 $n!$ 个排列对象的方式. 但是，不是所有的排列都产生 S_n 的不同元素. 考虑出现在 (7.13)中 e_j 个 j 次轮换 ($1\leqslant j\leqslant n$). 首先，这 e_j 个轮换可以用 $e_j!$种方式在它们中间置换，而不会改变所得出的 S_n 的元素；其次，每一轮换

$$(a_1a_2 \cdots a_j)$$

可以用 j 个不同方式写出，因为

$$(a_1\, a_2 \cdots a_j)=(a_2\, a_3 \cdots a_j\, a_1)=\cdots=(a_j\, a_1 \cdots a_{j-1}).$$

因而就 j 次轮换而论，S_n 的每一元素共计算了 $e_j!j^{e_j}$次. α 共轭类的一个特殊元素总共重复了 $1^{e_1}e_1!2^{e_2}e_2!\cdots n^{e_n}e_n!$次. 因而在这类中不同元素的个数由 (7.12)给定.

从命题 7 (§ 17) 我们知道 h_α是群S_n中α的中心化子的指数. 因而我们有下面的结果.

命题23 假如 α 是具有轮换类型 (7.11)的置换，那么 α 在 S_n 中的中心化子的阶是

$$1^{e_1}e_1!2^{e_2}e_2!\cdots n^{e_n}e_n!. \tag{7.14}$$

例 设 ϕ 是一包含 n 个对象的轮换，比如说

$$\phi=(1\ 2\ \cdots\ n).$$

在这情况中 $e_1=e_2=\cdots=e_{n-1}=0, e_n=1$. 因而由 (7.14)，$\phi$ 的中心化子是 n 阶的. 但是 ϕ 肯定与 $\iota(=\phi^0), \phi, \phi^2, \cdots, \phi^{n-1}$交换，它们是 S_n 的 n 个不同元素. 因而在这情况中，ϕ 的中心化子与 ϕ 所生成的循环群重合.

§ 40. 对换. 2 次轮换称为**对换**. 因而典型的对换，比如说

$$\tau=(ab) \tag{7.15}$$

交换 a 与 b 而保持所有其他元素不变. 我们注意

$$\tau^2=\iota,\quad \tau=\tau^{-1},$$

此处 ι 是恒等置换. 群 S_n 共包含$\frac{1}{2}n(n-1)$ 个对换.

下面，我们令 S_n 作用在一组未定元

$$x_1, x_2, \cdots, x_n \tag{7.16}$$

上，假设 α 将 i 置换成 a_i，我们定义

$$x_i\alpha=x_{a_i}\quad (i=1,2,\cdots,n).$$

更一般地，假如 f 是未定元(7.16)的任一函数，我们令

$$f(x_1,x_2,\cdots,x_n)\alpha=f(x_{\alpha_1},x_{\alpha_2},\cdots,x_{\alpha_n}).\qquad(7.17)$$

特别，我们考虑差积

$$\Delta=\prod_{i<j}(x_i-x_j)=(x_1-x_2)(x_1-x_3)(x_1-x_4)\cdots(x_1-x_n)$$
$$\times(x_2-x_3)(x_2-x_4)\cdots(x_2-x_n)$$
$$\times(x_3-x_4)(x_3-x_5)\cdots(x_3-x_n)\cdots$$
$$\times(x_{n-1}-x_n)\qquad(7.18)$$

显然，假如未定元受到置换 α 的作用，则函数Δ或者保持不变或者乘以(-1). 因而在(7.17)的符号中

$$\Delta\alpha=\zeta(\alpha)\Delta,\qquad(7.19)$$

此处$\zeta(\alpha)=\pm1$.

定义 10 置换 α 按照 $\zeta(\alpha)=1$ 或 $\zeta(\alpha)=-1$ 称为**偶置换**或**奇置换**，函数 $\zeta(\alpha)$ 称为S_n的**交错特征标**.

关于这函数的最重要的事实用下面的命题表出.

命题 24 假如 α 与 β 是任意的置换，那么

$$\zeta(\alpha\beta)=\zeta(\alpha)\zeta(\beta)\qquad(7.20)$$

即两个偶置换或两个奇置换的积是偶置换，而一个偶置换与一个奇置换的积是奇置换.

证明 我们应用运算β到(7.19)的两边，注意根据运算合成的定义，有

$$(\Delta\alpha)\beta=\Delta(\alpha\beta).$$

因而

$$\Delta(\alpha\beta)=\zeta(\alpha)\Delta\beta,$$

常数 $\zeta(\alpha)$没有受到β作用的影响. 应用(7.19)到 $\alpha\beta$ 与 β，我们得到关系式

$$\zeta(\alpha\beta)\Delta=\zeta(\alpha)\zeta(\beta)\Delta,$$

从而得出结论. 更一般地，有

$$\zeta(\alpha_1\alpha_2\cdots\alpha_r)=\zeta(\alpha_1)\zeta(\alpha_2)\cdots\zeta(\alpha_r).\qquad(7.21)$$

$\zeta(\alpha)$的定义可以改写得使函数 Δ 不明显出现. 每一Δ的因子(x_i-x_j)对应一整数对 (i,j),使得 $1\leqslant i<j\leqslant n$. 设 α 使 i 成为 a_i,使 j 成为 a_j,在应用 α 之后,(x_i-x_j) 变成$(x_{a_i}-x_{a_j})$. 假如 $a_i<a_j$,则它是 Δ 的因子,假如 $a_i>a_j$,则 Δ 包含因子 $-(x_{a_i}-x_{a_j})$. 假如 $i-j$ 与 a_i-a_j 符号相反,我们说对 (i,j) 带来一逆序. 当考虑到所有的对(i,j)时,设 t 是逆序的总数,那么

$$\zeta(\alpha)=(-1)^t.$$

数字 t 易于用如下方法找到:将置换 α 写成标准形式,例如

$$\alpha=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{pmatrix}$$

$$\| \quad \| \quad \||| \quad | \quad | \qquad (t=9)$$

设 k 是第二行的任一数. 假如 k 被 $s(\geqslant 0)$ 个小于 k 的整数跟随,我们就说 k 有 s 分. 对每一 k 记分,从而总分 t 易于找出. 例如,3 有两分,因为它被 2 与 1 跟随,而 6 有 3 分,因为它被 2,5 与 1 跟随. 在这例中 $t=9$,所以 $\zeta(\alpha)=-1$.

显然,恒等置换 ι 使 Δ 不变,因此

$$\zeta(\iota)=1. \tag{7.22}$$

其次,对任一置换 α,

$$\zeta(\alpha)\zeta(\alpha^{-1})=\zeta(\iota)=1,$$

从而

$$\zeta(\alpha)=\zeta(\alpha^{-1}), \tag{7.23}$$

即逆置换具有相同的交错特征标.

假如 α 与 β 是任意的置换,则

$$\zeta(\beta^{-1}\alpha\beta)=\zeta(\beta^{-1})\zeta(\alpha)\zeta(\beta)=\zeta(\alpha),$$

因而共轭置换具有相同的特征标,即在 S_n 的每一共轭类上,ζ 是常数.

象在(7.15)中那样，设 τ 是某一对换，那么由命题21，τ 与特殊对换 $\sigma=(12)$ 共轭. σ 的作用改变了 (x_1-x_2) 的符号，且用(7.18)中第二行的因子与第一行的其他因子交换，并不引进更多的负号，因而 $\zeta(\sigma)=-1$，因此 $\zeta(\tau)=-1$. 因而所有对换是奇置换.

为了找到 m 次轮换的特征标，我们利用公式

$$(a_1a_2\cdots a_m)=(a_1a_2)(a_1a_3)\cdots(a_1a_m). \tag{7.24}$$

通过计算右边的积容易证明这公式，即

$$a_1\to a_2,\ a_2\to a_1\to a_3,\ a_3\to a_1\to a_4,\text{等等.}$$

因为(7.24)包含 $m-1$ 个对换因子，因此我们有

$$\zeta(a_1a_2\cdots a_m)=(-1)^{m-1}. \tag{7.25}$$

下面(7.24)的推论值得写下.

定理 21 每一置换能够用许多方式表示为对换的积. 在任一这样的积中，对换因子的个数按照给定的置换是偶置换或奇置换而总为偶数或奇数.

证明 设 α 是给定的置换. 我们已经知道(§7)α 可以表成轮换的积. 根据(7.24)，每一轮换是对换的积，因而我们肯定有

$$\alpha=\tau_1\tau_2\cdots\tau_s. \tag{7.26}$$

此处每一 τ 是一对换，这乘积不是唯一的，例如我们能嵌入一对因子

$$(ab)(ba),$$

它等价于恒等置换. 较难看出的是，假如 $a\neq1$ 与 $b\neq1$，我们有关系式

$$(ab)=(1\,a)(1\,b)(1\,a). \tag{7.27}$$

当其中对象1被与 a 和 b 不同的任一对象所代替时，也存在类似的关系. 可是，(7.26)意味 $\zeta(\alpha)=(-1)^s$，因为 $\zeta(\alpha)$ 只由 α 决定，因此按照 α 是偶置换或奇置换，s 就是偶数或奇数。

利用 §12 中引入的术语我们有

推论 群 S_n 由一组对换所生成.

利用(7.27),这结论可以变得更精确.

命题 25 群 S_n 由 $n-1$ 个对换

$$(1\ 2),(1\ 3),\cdots,(1n)$$

所生成.

§ 41. 交代群. 我们回来讨论定义 10 中所引入的偶置换与奇置换之间的区别. 我们从一个关于任一置换群的简单结果开始,这个置换群是对于某一合适的 n 值的 S_n 的任一子群.

命题 26 在每一置换群 G 中,偶置换形成一个正规子群,它或者等于 G 或者在 G 中的指数是 2.

证明 设 H 是 G 中偶置换的集.由(7.20),(7.22)与(7.23), H 是 G 的子群. 假如 $H=G$,我们就没有什么可证明的. 假如 $H\neq G$,那么G 至少包含一个奇置换σ,而陪集 $H\sigma$ 与H不同. 设 δ 为 G 的任一奇置换,那么$\sigma\delta^{-1}$ 是偶置换,即$\sigma\delta^{-1}\in H$, $H\sigma=H\delta$ (§ **10**.命题 5). 因而 G 中只有两个 H 的陪集,所以$[G:H]=2$,象所断定的那样. 根据 § **19** 末尾的(iv),H 在 G 中是正规的.

我们特别对 $G=S_n$ 的情况感兴趣.

定义11 S_n 的所有偶置换的集($n\geqslant 2$)形成$\frac{1}{2}n!$ 阶的群 A_n,称为 n 次**交代群**.

例如,群 A_4 是$\frac{1}{2}(4!\ )=12$ 阶的,由下列置换(按照 S_4 的共轭类排列)组成

$$A_4=C_0\cup C_1\cup C_2,$$

此处$C_0=\iota$

$$C_1=(12)(34)\cup(13)(24)\cup(14)(23) \tag{7.28}$$

$$C_2=(123)\cup(124)\cup(132)\cup(134)\cup(142)$$
$$\cup(1\ 4\ 3)\cup(2\ 3\ 4)\cup(2\ 4\ 3).$$

我们可以问除了 A_n 以外，S_n 是否还有其他正规子群. 不讨论 $n=1$ 或 $n=2$ 时的平凡情况，当 $n=3$ 或 $n=4$ 时我们将从最初等的原则出发，利用以下事实来回答这问题：正规子群必须是共轭类的并集，其中包含单位元素组成的类(见 § 19 末尾的 (iii)).

S_3 的类是

$$\iota, (12)\cup(13)\cup(23) \text{及} (123)\cup(132),$$

分别含有 1 个，3 个与 2 个元素. 只有当我们将单位元素与最后一类合并才得到一个元素个数可以除尽 $|S_3|$ $(=6)$ 的集，对于子群这是必须的. 事实上，

$$A_3=\iota\cup(123)\cup(132),$$

因此这是 S_3 的唯一真正规子群.

群 S_4 具有五个共轭类(见 § 39 表 (xiii)). 其中三类由偶置换组成的列举在(7.28)中，剩下的两类是

$$C_3=(12)\cup(13)\cup(14)\cup(23)\cup(24)\cup(34) \text{及}$$

$$C_4=(1234)\cup(1243)\cup(1324)\cup(1342)\cup(1423)\cup(1432)$$

因为 $|C_0|=1$, $|C_1|=3$, $|C_2|=8$, $|C_3|=1$, $|C_4|=6$, 只有

$$V=C_0\cup C_1 \qquad \text{及} \qquad A_4=C_0\cup C_1\cup C_2$$

具有能整除 $|S_4|$ $(=24)$ 的基数，这对于子群是需要的. 我们已经知道 $A_4\triangleleft S_4$，值得注意的是

$$V=\iota\cup(12)(34)\cup(13)(24)\cup(14)(23)$$

碰巧是群. 因为我们令 $\alpha=(12)(34)$ 及 $\beta=(13)(24)$，那么 $\alpha\beta=\beta\alpha=(14)(23)$ 及 $\alpha^2=\beta^2=\iota$. 因而 $V\triangleleft S_4$，而 V 具有四群 (§ 14) 的结构. 我们于是已经证明 A_4 与 V 是 S_4 的仅有的真正规子群. 附带说一句，因为 V 只包含偶置换，我们有 $V\triangleleft A_4$.

在合成列(§ 35)

$$S_3\triangleright A_3\triangleright\{1\}, \quad S_4\triangleright A_4\triangleright V\triangleright\{1\}^*$$

中，所有的合成因子都是素数阶，这证明 S_3 与 S_4 都是可解群

* 原书此处有误，应为 $S_4\triangleright A_4\triangleright V\triangleright B\triangleright\{1\}$，其中 $B=\iota\cup(12)(34)$.

(§ 36). 过一会我们将看到，当 $n>4$ 时 S_n 在这方面的性态不一样.

对群 A_n 我们选择一组相当简单的生成元是有用的.

命题 27 当 $n\geqslant 3$ 时，群 A_n 能为 $n-2$ 个三元轮换

$$(123),(124),\cdots,(12\,n) \tag{7.29}$$

所生成

证明 由命题 25，每一置换能表成形状为$(1\,i)$的对换的积. 对于偶置换，对换因子的个数一定是偶数，因而 A_n 为因子对$(1\,i)(1\,j)$等所生成. 因为$(1\,i)^2=\iota$，我们可以假定在每一因子对中 $i\neq j$. 现在

$$(1\,i)(1\,j)=(1\,ij). \tag{7.30}$$

假如 $i=2$，这一对对换等于列举在(7.29)中的某一三元轮换. 假如 $j=2$，我们看出

$$(1\,i)(12)=(1\,i\,2)=(12\,i)^2.$$

最后假如 $i>2$ 及 $j>2$，我们利用关系式

$$(1\,ij)=(12\,j)(12\,i)(12\,j)^{-1}.$$

因而在所有情况下，(7.30)的右边都能用(7.29)的生成元表示出来.

我们回忆一下单群(§ 19)的概念，马上就来证明关于交代群的一个有名的结果，它是由 E·伽罗瓦得到的.

定理 22 当 $n\neq 4$ 时，群 A_n 是单群.

证明 我们已经知道 V 是 A_4 的真正规子群，因而 A_4 不是单群. 从现在起我们将假定 $n>4$. 这定理等于说：假如 $N\lhd A_n$ 及 $|N|>1$，那么 $N=A_n$. 关键性的假设是 N 在 A_n 中是正规的. 因而假如 $\alpha\in N$，又假如 δ 是任一偶置换，那么 $\delta^{-1}\alpha\delta\in N$，因而也有 $\delta^{-1}\alpha\delta\alpha^{-1}\in N$. 这定理的证明分成几步.

(i) 假定 N 包含一个 3-轮换. 比如说

$$\alpha=(abc).$$

我们将证明 N 包含所有 3-轮换

$$\xi=(xyz).$$

此处 x,y,z 是任意预先指定的不同对象. 由命题 27 这立即意味 $N=A_n$.

置换

$$\phi=\begin{pmatrix} a & b & c \\ x & y & z \end{pmatrix}$$

是 S_n 的元素,其中凡未在 ϕ 中提到的对象在 ϕ 的作用下是不变的. 由(7.6)我们有

$$\phi^{-1}\alpha\phi=\xi.$$

既然 $n\geqslant 5$,至少有两个对象 e,f 不包含在 α 内,对换 $\tau=(ef)$与 α 交换,于是

$$(\tau\phi)^{-1}\alpha(\tau\phi)=\xi.$$

显然,或者 ϕ 属于 A_n 或者 $\tau\phi$ 属于 A_n. 因而 α 在 A_n 中与 ξ 共轭,于是我们断定 $\xi\in N$.

(ii) 其次,我们假定 N 包含置换 ω

$$\omega=\gamma\delta\varepsilon\cdots, \tag{7.31}$$

此处 $\gamma,\delta,\varepsilon,\cdots$是不相交轮换,而 γ 的次数超过 3,比如说

$$\gamma=(a_1a_2a_3a_4\cdots a_m),m>3.$$

因为 $\sigma=(a_1a_2a_3)$是偶置换,它与(7.31)的所有轮换,除第一个之外,都是交换的. 因而

$$\omega_1=\sigma^{-1}\omega\sigma=(\sigma^{-1}\gamma\sigma)\delta\varepsilon\cdots$$

属于 N, 于是 $\omega_1\omega^{-1}$ 也属于 N. 因为$\delta,\varepsilon,\cdots$与 γ 及 $\sigma^{-1}\gamma\sigma$ 两元素都交换,我们得出

$$\begin{aligned}\omega_1\omega^{-1}&=\sigma^{-1}\gamma\sigma\gamma^{-1}=(a_2a_3a_1a_4\cdots a_m)(a_ma_{m-1}\cdots a_4a_3a_2a_1)\\&=(a_1a_3a_m).\end{aligned}$$

因而 N 包含一个 3-轮换，于是我们从(i)推导出 $N=A_n$. 从今以后我们可以假定N的所有置换是次数为 1,2 或 3 的不相交轮换的积.

(iii) 假设 N 包含一置换 ω，它至少含有两个 3-轮换，比如说

$$\omega=\alpha\beta\lambda,$$

此处 $\alpha=(a_1a_2a_3)$, $\beta=(b_1b_2b_3)$, 而 λ 与 a_i 或 b_i $(i=1,2,3)$ 无关. 选取

$$\sigma=(a_2a_3b_1),$$

我们看出 σ 与 λ 交换. 因而 N 包含元素

$$\begin{aligned}\sigma^{-1}\omega\sigma\omega^{-1}&=(\sigma^{-1}\alpha\sigma)(\sigma^{-1}\beta\sigma)\beta^{-1}\alpha^{-1}\\&=(a_1a_3b_1)(a_2b_2b_3)(b_3b_2b_1)(a_3a_2a_1)\\&=(a_1a_2b_1a_3b_3),\end{aligned}$$

这与次数大于 3 的轮换不会在N中出现的假设矛盾.

(iv) 当因子只有单独一个 3-轮换时，典型的元素具有形式

$$\omega=(a_1a_2a_3)\lambda,$$

此处 λ 是不相交对换的积，因而 $\lambda^2=\iota$，而 N 包含元素

$$\omega^2=(a_1a_3a_2),$$

这又使我们回到(i).

(v) 最后，我们必须讨论这种情况，即 N 的所有元素除 ι 之外，都是不相交对换的积. 当 $n=4$，这种情况实际上存在，并且就是前面所提到的群 V. 可是，因为我们假定 $n>4$，所以我们可以讨论如下：因为对换因子的个数必须是偶数，N的典型元素形状如下.

$$\omega=(a_1a_2)(b_1b_2)\lambda,$$

此处 λ 不包含 a_1,a_2,b_1,b_2. 选择第五个元素 c，它与刚才提到的元素不同，我们依次利用变换元素 $\sigma=(a_2b_1b_2)$ 及 $\delta=(a_1b_2c)$ 从 ω 来进一步构造N的元素如下：

$$\omega_1=\sigma^{-1}\omega\sigma=(a_1b_1)(b_2a_2)\lambda,$$
$$\omega_2=\omega_1\omega^{-1}=(a_1b_1)(b_2a_2)(b_1b_2)(a_1a_2)=(a_1b_2)(a_2b_1),$$
$$\omega_3=\delta^{-1}\omega_2\delta=(b_2c)(a_2b_1),$$
$$\omega_3\omega_2^{-1}=(b_2c)(a_2b_1)(a_2b_1)(a_1b_2)=(a_1b_2c).$$

因而，与我们的假设相反，N 终究包含了一个 3-轮换，这就结束了本定理的证明.

我们现在可以回到当 $n>4$ 时关于 S_n 的正规子群的问题.

命题 28 当 $n>4$，S_n 的唯一真正规子群是交代群 A_n.

证明 假定 $H\lhd S_n$ 及 $|H|>1$. 首先，我们将证明 H 不能是 2 阶群，因为假如

$$H=\{\iota,\xi\mid\xi^2=\iota\}$$

那么 ξ 必须或者是对换，或者是不相交对换的积，在前一种情况，设 $\xi=(ab)$，存在对象 c，与 a 和 b 不同. 因为 $H\lhd S_n$，元素 $(ac)^{-1}(ab)(ac)=(bc)$就属于 H，H 就要包含多于 2 个的元素. 其次，假设 $\xi=(a_1a_2)(b_1b_2)\lambda$，此处 λ 与 a_1,a_2,b_1,b_2 无关. 那么，假如 $\sigma=(a_2b_1b_2)$，$\sigma^{-1}\xi\sigma\in H$，但 $\sigma^{-1}\xi\sigma\neq\xi$，这与假设 $|H|=2$ 矛盾. 因而 $|H|>2$. 由命题 26，H 的元素至少有一半是偶置换. 因而，假如 $D=H\cap A_n$，那么 $|D|>1$. 显然 $D\lhd A_n$. 因为 A_n 是单群，所以 $D=A_n$，这意味着

$$A_n\leqslant H. \tag{7.32}$$

由于 H 是 S_n 的真子群，我们有 $|H|\leq\frac{1}{2}n!$. 因而 $|A_n|=|H|$，而我们从(7.32)断定 $A_n=H$.

§ 42. 置换表示. 一直到二十世纪初，群的抽象概念才充分地为数学家所重视和接受. 关于群论较早的文献，包括哥西，伽罗瓦与 C. 约当的经典著作在内，几乎都专门讨论置换群，即对称群 S_n 的子群. 可是，它们的许多结果同样好地应用到任意有限群，而不依

赖群的元素是置换这假设．即使在近代群论的范围内，置换群的研究也是十分有趣的问题．不仅这些群提供了有限群的大量的十分容易理解的例子，而且，象 A. 凯莱在 1854 年所讲过的那样，每一有限群与某一置换群同构．

设

$$G: a_1, a_2, \cdots, a_g \tag{7.33}$$

是 g 阶有限群．假如 x 是其中任一元素，积

$$a_1x, a_2x, \cdots, a_gx \tag{7.34}$$

是 G 的 g 个不同元素．因而构成整个群．因此(7.34)是(7.33)的重新排列，即我们能够将下面的 g 次置换与 x 相联系

$$x\rho = \begin{pmatrix} a_1 & a_2 & \cdots a_g \\ a_1x & a_2x & \cdots a_gx \end{pmatrix}.$$

这置换所作用的对象是群本身的元素．利用下面缩写的记号是方便的：

$$x\rho = \begin{pmatrix} a_i \\ a_ix \end{pmatrix} (i=1,2,\cdots,g). \tag{7.35}$$

$x\rho$ 在 G 上的作用可以简短地说成对 G 的每一元素在右边乘以 x．元素排列的次序是不重要的．特别，假如 u 是 G 的固定元素，那么象我们在(7.34)中已经讲过的那样，积 $a_iu(i=1,2,\cdots,g)$ 是 G 的所有元素．因此，我们能写

$$x\rho = \begin{pmatrix} a_iu \\ a_iux \end{pmatrix}. \tag{7.36}$$

现在设 y 是 G 的另一元素，设

$$y\rho = \begin{pmatrix} a_i \\ a_iy \end{pmatrix} \tag{7.37}$$

是与 y 相联系的置换．计算置换(7.35)与(7.37)的积，利用(7.36)我们得出

$$(x\rho)(y\rho)=\begin{pmatrix}a_i\\a_ix\end{pmatrix}\begin{pmatrix}a_i\\a_iy\end{pmatrix}=\begin{pmatrix}a_i\\a_ix\end{pmatrix}\begin{pmatrix}a_ix\\a_ixy\end{pmatrix}=\begin{pmatrix}a_i\\a_ixy\end{pmatrix}$$

因而

$$(x\rho)(y\rho)=(xy)\rho, \tag{7.38}$$

这证明了映射

$$\rho: G\to S_g$$

是G到S_g内的同态. 此外,ρ是单的,即它的核仅仅包含G的单位元素1（§ **21**,命题9）. 因为假如

$$x\rho=\iota,$$

即S_g的单位元素,这意味着

$$a_ix=a_i \quad (i=1,2,\cdots,g),$$

这明显地意味$x=1$. 事实上,假如$x\neq 1$,$x\rho$就置换了G的每一元素. 因为ρ是单的,所以G在ρ下的象与S_g的某一子群同构.

其次,我们将分解$x\rho$成不相交轮换. 设x是r阶的,那么

$$x^r=1. \tag{7.39}$$

从G的任一元素a开始,我们知道$x\rho$的作用是将a变成ax,而ax依次变成ax^2,ax^2的象是ax^3,等等,一直到ax^{r-1}为止,ax^{r-1}的象由(7.39)等于a. 因而$x\rho$包含轮换

$$(a,ax,ax^2,\cdots,ax^{r-1}), \tag{7.40}$$

它含有G的r个不同元素. 假如$r<g$,我们选择不含在(7.40)中的元素b,我们又能构成另一个轮换

$$(b,bx,bx^2,\cdots,bx^{r-1}). \tag{7.41}$$

显然,(7.40)与(7.41)没有公共元素. 因为,假如它们有公共元素,那么$b=ax^t(0\leqslant t\leqslant r-1)$,这与$b$的选择矛盾. 我们如此继续建立轮换,每一轮换包含$r$个元素,直到$G$的$g$个元素都包含在这些轮换内. 因而,比如说

$$x\rho=(a,ax,\cdots,ax^{r-1})(b,bx,\cdots,bx^{r-1})\cdots (f,fx,\cdots,fx^{r-1}).$$

所有轮换都具有相同长度的置换称为**正则置换**. 附带说一句，最后的式子断定 r 是 g 的因子.

我们总结以上结果如下：

定理 23(凯莱) 设 G：$a_1, a_2, \cdots, a_g$ 是 g 阶抽象群，对 G 的每一元素 x 我们联系一个正则置换

$$x\rho=\begin{pmatrix} a_1 & a_2 & \cdots & a_g \\ a_1x & a_2x & \cdots & a_gx \end{pmatrix},$$

这样定义的映射 $\rho: G\to S_g$ 是单同态，所以 G 与 S_g 的某一子群同构. 假如 x 是 r 阶的，那么 $x\rho$ 是 g/r 个 r 次轮换的积.

当抽象群 G 与群 G' 同构，而 G' 的元素是具体的数学实体，例如置换或矩阵时，我们根据情况说 G' 是 G 依据置换或矩阵的**忠实表示**. G 的所有性质 G' 也都具有. 反之，关于 G' 的任何不依赖其元素特殊性质的事实，同样地适用于 G. 由于用具体元素实现计算通常更为方便，因而表示的存在使我们能够阐明抽象群的构造. 这方法类似于利用坐标讨论几何问题. 由凯莱定理所提供的特殊表示称为 G 的**右正则表示**. 当 G 用乘法表(§ 4)给出时，右正则表示可以立即看出来：在 $x\rho$ 的两行符号中顶上一行是乘法表中用1领头的一列，底下一行是乘法表中用 x 领头的一列. 给出；右正则表示实际上等于给出乘法表的构造.

例 在 § 4 表(v)给出的 6 阶非阿贝尔群中，右正则表示的元素分解成许多轮换如下：

$$1\rho=\begin{pmatrix} 1 & a & b & c & d & e \\ 1 & a & b & c & d & e \end{pmatrix}=(1)(a)(b)(c)(d)(e),$$

$$a\rho=\begin{pmatrix} 1 & a & b & c & d & e \\ a & b & 1 & d & e & c \end{pmatrix}=(1ab)(cde),$$

$$b\rho=\begin{pmatrix} 1 & a & b & c & d & e \\ b & 1 & a & e & c & d \end{pmatrix}=(1ba)(ced),$$

$$c\rho=\begin{pmatrix}1&a&b&c&d&e\\c&e&d&1&b&a\end{pmatrix}=(1\,c)(ae)(bd),$$

$$d\rho=\begin{pmatrix}1&a&b&c&d&e\\d&c&e&a&1&b\end{pmatrix}=(1\,d)(ac)(be),$$

$$e\rho=\begin{pmatrix}1&a&b&c&d&e\\e&d&c&b&a&1\end{pmatrix}=(1\,e)(ad)(bc).$$

有时把右正则表示的典型元素写成 ρ_x 而不写成 $x\rho$ 更为方便. 因而 ρ_x 可以简明地用下面的公式描写：

$$a\rho_x=ax\quad(a\in G).\tag{7.42}$$

更一般地，我们可以考虑同态

$$\theta:G\to S_n.$$

它不需要是单的(忠实的)，其中 n 是适当的整数. 当这样的同态存在时，我们说 G 具有 n 次的**置换表示**. 下面是构造这种表示的相当一般的方法：设 H 是 G 的子群，又设

$$G=Ht_1\cup Ht_2\cup\cdots\cup Ht_n\tag{7.43}$$

是 G 的关于 H 的右陪集的分解式，此处 $n=[G:H]$（见 § 10）. 假如 x 是 G 的固定元素，右陪集 $Ht_ix(i=1,2,\cdots,n)$ 是不同的，因此必与列举在(7.43)中的右陪集相同，因而

$$x\theta=\begin{pmatrix}Ht_1&Ht_2&\cdots&Ht_n\\Ht_1x&Ht_2x&\cdots&Ht_nx\end{pmatrix}$$

是 n 次的置换，置换的对象是 n 个 H 在 G 中的右陪集. 利用类似于本节开头所用过的论证，容易证明 θ 是同态，即

$$(x\theta)(y\theta)=(xy)\theta.$$

假如 k 在 θ 的核内，我们必有

$$Ht_ik=Ht_i\quad(i=1,2,\cdots,n),$$

它等价于条件 $t_ik\in Ht_i$ 或者 $k\in t_i^{-1}Ht_i(i=1,2,\cdots,n)$. 可是任一与 H 共轭的子群具有 $t_i^{-1}Ht_i$ 的形式，其中 i 取某一合适的值，因为假如 y 是 G 的任一元素，它位于某一个陪集内，例如 $y\in Ht_{i_0}$，即 $y=$

ut_i，此处$u\in H$. 那么$y^{-1}Hy=t_i^{-1}u^{-1}Hut_i=t_i^{-1}Ht_i$. 因而我们可以说$\theta$的核由所有与$H$共轭的群的交集组成. 我们将这些结果搜集到下面的定理中.

定理 24 设H是G的子群，具有有限指数n，设$t_1,t_2,\cdots,t_n$是H在G中的横截(§ 10)，我们将G的每一元素x与下面的置换相联系

$$x\theta=\begin{pmatrix}Ht_1 & Ht_2 & \cdots & Ht_n\\ Ht_1x & Ht_2x & \cdots & Ht_nx\end{pmatrix}.$$

照这样所定义的映射$\theta:G\rightarrow S_n$是同态，θ的核由所有与H共轭的群的交集组成.

我们用一个例子来结束本节，这个例子说明如何用这些概念来得到关于群的结构的知识.

例 交代群A_5没有阶为30，20或15的子群. 换句话说，我们断定假如H是A_5的真子群，那么$[A_5:H]\geqslant5$. 假设H是真子群，令$[A_5:H]=n$. 由定理 24，存在同态$\theta:A_5\rightarrow S_n$. 设$K$是$\theta$的核，我们知道(§ 21)$K$是$A_5$的正规子群. 但$A_5$是单群(定理 22). 因而或者$K=\{1\}$或者$K=A_5$. 后一种可能性立即被排除，因为由定理24，$K$包含在$H$中，因此$|K|\leqslant|H|<|A_5|$. 因此我们必须有$K=\{1\}$，即$\theta$是单射. 因而$A_5$在$\theta$下的象包含60个$S_n$的不同元素，而这是不可能的，除非$n\geqslant5$.

§ 43. 可迁群. 在本节与下节，我们考虑次数固定的置换，即我们讨论某一特殊对称群S_n的子群G. G所作用的对象将以$1,2,\cdots,n$或字母$a,b,\cdots$表示.

定义 12 置换群称为**可迁群**，假如给定任一对字母a,b(它们不需要不相同)，群中至少存在一置换，它将a变换到b；否则这群称为**非可迁群**.

应该注意这概念只适用于置换群.

将a变换成b的置换将以θ_{ab}表示，不考虑它在其他对象上

的效果，当然，对于给定的一对 a,b，可能有很多这样的置换.我们注意 θ_{ab}^{-1} 将 b 改变成 a.

显然，对称群 S_n 是可迁群，因为它包含所有可能的置换，其中包括对换 (a,b) 它可以当作 θ_{ab}.

在另一方面，4 阶的 4 次群

$$V_1:(1),(12),(34),(12),(34)$$

是非可迁的，因为它没有将 1 转变成 3 的置换，附带指出，这群与下面的群同构.

$$V_2:(1),(12)(34),(13)(24),(14)(23).$$

恰好相反，V_2 是可迁群. 这两个群都与四群（§ **4**，表 (iii)）同构.

G 中保留符号 1 不变的置换集形成子群 G_1；因为恒等变换肯定属于 G_1，G_1 的任意元素的逆元素以及任意两个元素的积也属于 G_1. 我们称 G_1 为 1 的**稳定化子**，对象 a 的稳定化子也类似地定义.

定理 25 n 次置换群 G 是可迁的，当且仅当稳定化子 G_1 在 G 中的指数是 n.

证明 (1) 假如 G 是可迁的，根据假定，G 包含置换

$$\theta_{11},\theta_{12},\cdots,\theta_{1n}, \tag{7.44}$$

它们分别将 1 变换成 $1,2,\cdots,n$，右陪集

$$G_1\theta_{11},G_1\theta_{12},\cdots,G_1\theta_{1n} \tag{7.45}$$

彼此是不相同的，因为 $G_1\theta_{1i}$ 的所有元素将 1 变换成 i，因此当 $i\neq j$ 时，它与 $G_1\theta_{1j}$ 的元素不同，尚需证明(7.45)是全部陪集，设 ξ 是 G 的任一元素，假设 ξ 将 1 变换成 a，那么 $\xi\theta_{1a}^{-1}$ 使1不变，即 $\xi\theta_{1a}^{-1}\in G_1$，因而 $\xi\in G_1\theta_{1a}$. 这证明陪集(7.45)的并集是整个群，因而 $[G:G_1]=n$.

(ii) 反之，假设 G_1 的指数是 n，并设

$$G=G_1\tau_1\cup G_1\tau_2\cup\cdots\cup G_1\tau_n$$

是 G 关于 G_1 的陪集分解．首先，置换

$$\tau_1, \tau_2, \cdots, \tau_n \tag{7.46}$$

中没有两个在对象1上有相同的效果．因为假如τ_i与 τ_j 两个置换都将1变换成a，那么$\tau_i\tau_j^{-1}$使 1 不变，因此$\tau_i\tau_j^{-1}\in G_1$，于是 $G_1\tau_i=G_1\tau_j$（§ **10**，命题 5）．除非 $i=j$，否则这是不可能的．因而我们能在某种排列次序下把置换(7.46) 取作置换(7.44)．将(7.46) 这样排列使$\theta_{1i}=\tau_i(i=1,2,\cdots,n)$是方便的．最后，假如 a,b 是任一对符号，$\tau_a^{-1}\tau_b$将a变换成 b，这就证明了 G 是可迁的．

因为有限群的阶可以被它的任一子群的指数除尽(§ **10**，定理 3)，我们有下面有用的推论．

命题 29 *n次可迁群的阶可被n整除．*

可迁性概念可以推广．

定义 13 *置换群G称为k重可迁的，假如它至少包含一置换θ，将任意一个由k个不同对象 $a_1,a_2,\cdots,a_k$ 组成的有序集变换成另外任意这样的集 $b_1,b_2,\cdots,b_k$（这两个集可以有相同元素），即 $a_i\theta=b_i(i=1,2,\cdots,k)$．*

显然，假如G 是n 次，那么 $k\leqslant n$．同样，假如 G是k重可迁的，以及假如$l<k$，那么G更是l重可迁的．

群 S_n 是 k 重可迁的，此处 k 是整数 $1,2,\cdots,n$ 中的任一个．

设v是包含k 个对象的有序集的个数，这 k 个对象是从所有 G 所作用的 n 个对象中挑选出来的，那么

$$v=n(n-1)\cdots(n-k+1).$$

现在假设 G是 k 重可迁的，又设 H 是子群，它使下面的每一个对象固定不变

$$1,2,\cdots,k.$$

利用与定理 25中的证明相似的证法可以证明H在G中的指数等于v，H的陪集与v个包含k个对象的集一一对应．因而我们有下述结

果：

定理 26 n 次 k 重可迁群的阶可被 $n(n-1)\cdots(n-k+1)$ 整除。

另外，我们可以利用下面的判别准则归纳地发展多重可迁性概念。

命题 30 假如(i) 群 G 是可迁的(ii) 稳定化子 G_1 关于对象 $2,3,\cdots,n$ 是 $k-1$ 重可迁的，则群 G 是 k 重可迁的。

例如，在 A_4 的情况中（A_4 已表示在(7.28)中），1 的稳定化子是

$$G_1: \iota, (234), (243),$$

因而 $[A_4:G_1]=12/3=4$，这就肯定 A_4 是可迁的。现在 G_1 在 2,3,4 上是可迁的，这可以直接证明，或者从下面的讨论中得出，因为 G_1 中2的稳定化子 G_{12} 退化到 ι，因此 G_{12} 在 G_1 中的指数是 3。又因为 G_{12} 在其余的对象 3,4 上不是可迁的，我们断定 A_4 恰好是双重可迁的。

§ 44. 本原群. 设 G 是可迁群，又设 G 所作用的 n 个对象可以排列成 r 行与 s 列的阵列

$$\left.\begin{array}{l} a_1, a_2, \cdots, a_s \\ b_1, b_2, \cdots, b_s \\ \cdots\ \cdots\ \cdots \\ k_1, k_2, \cdots, k_s \end{array}\right\} r \text{ 行} \qquad (7.47)$$

此处 $rs=n(r>1, s>1)$，这样的排列使得 G 的置换或者将同行中对象在它们中间重新排列，或者将一行的对象与另一行的对象交换(按某种次序)。因而位于(7.47)中不同行的两个对象决不会变换成同一行的对象，反之，同一行的两个对象也决不会在 G 的作用下变换到两个不同的行中去，具有这种性质的可迁群叫**非本原**的，而表(7.46) 称为**非本原系**。不存在非本原系的群称为**本原**的。我们应该注意这概念只适用于可迁群。

例 1 由置换

$$\iota,(1234),(13)(24),(1432)$$

所组成的循环群 $G=\mathrm{gp}\{(1234)\}$是非本原的，具有非本原系

$$\begin{array}{cc|}1&3\\2&4\end{array}\,.$$

事实上，G 的四个置换分别将这系变成

$$\begin{array}{cc|}1&3\\2&4\end{array}\,,\begin{array}{cc|}2&4\\3&1\end{array}\,,\begin{array}{cc|}3&1\\4&2\end{array}\,,\begin{array}{cc|}4&2\\1&3\end{array}\,.$$

例 2 一个群可以具有不止一个非本原系，例如在四群

$$\iota,(12)(34),(13)(24),(14)(23)$$

的情况中，每一阵列

$$\begin{array}{cc|}1&2\\3&4\end{array}\,,\begin{array}{cc|}1&3\\2&4\end{array}\,,\begin{array}{cc|}1&4\\2&3\end{array}$$

都可作为一个非本原系.

双重可迁群总是本原的. 因为双重可迁群一定含有一个置换，它将一对a_1,a_2变换成另一对a_1,b_2。可是这与存在象(7.47)那样的非本原系是不相容的.

特别，所有对称群S_n都是本原的.

§ 45. 图形的对称群. 令Σ是位于以O为原点的三维欧几里得空间中的有限或无限点集，围绕通过O点的轴的任一旋转将Σ变换到本身，称为Σ相对O的对称.

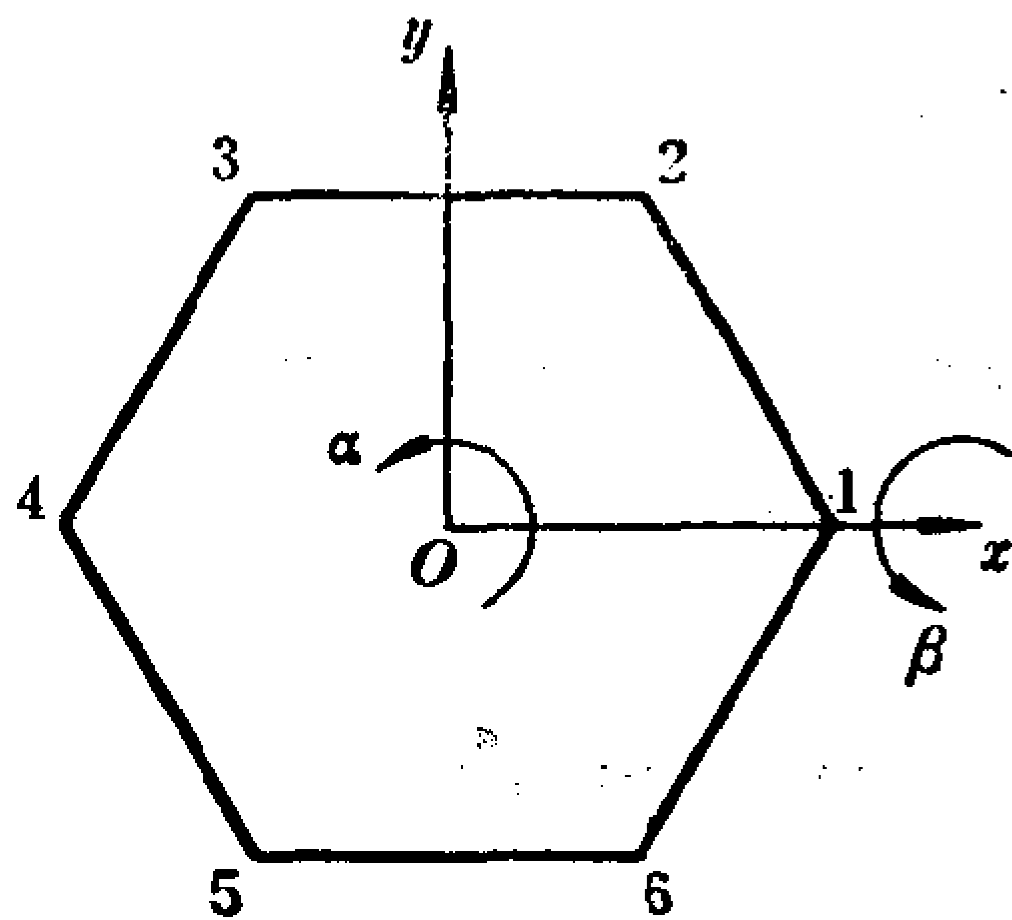


图 3

由第一章 § 6(例2)，Σ的对称在映射的合成下形成一个群. 假如不存在非平凡旋转使Σ与本身重合，那么这一对称群退化到恒等变换.

本节中，我们将讨论某些几何图形，包括五个正多面体的图形的对称群，这些群已为我们所知.

(i) **二面体群.** 考虑形为具有 n 个顶点的正多边形的平面薄片，假设薄片的两面完全一样(图 3 说明 $n=6$ 的情况)，我们这样选择坐标轴，使得薄片位于(x,y)-平面，中心在原点，x 轴通过某一顶点，以 1 标示之. 包括恒等运算在内，共有 $2n$ 个旋转使得薄片与它自身重合. 首先，假如 α 表示围绕 z 轴旋转 $2\pi/n$ 角，我们有 n 个对称运算.

$$\iota(=\alpha^0),\alpha,\alpha^2,\cdots,\alpha^{n-1},$$

此处

$$\alpha^n=\iota. \tag{7.48}$$

另一个对称运算β是颠倒薄片的两面. 这可以用绕x轴转动 π 角的旋转来完成(假设 x 轴在空间固定). 显然

$$\beta^2=\iota, \tag{7.49}$$

因为 β^2 对应于旋转 2π 角，因此等于恒等运算. 于是 $2n$ 个运算

$$\alpha^k\beta^l(k=0,1,\cdots,n-1;\ l=0,1)$$

构成薄片的所有对称：因为它们将任一个顶点带到另一个顶点的位置，薄片的两个面可以颠倒也可以不颠倒. 为了决定这个图形的对称群的结构，我们必须找出 α 与 β 之间的关系. 一个简单的几何上的考察表明

$$\alpha\beta=\beta\alpha^{-1},$$

由于(7.49)，它相当于

$$(\alpha\beta)^2=\iota. \tag{7.50}$$

(建议读者画一个类似 § 3 中的图来证实这等式.) 我们的结果可以总结如下.

正 n 边形薄片的对称群是由定义关系

$$\alpha^n=\beta^2=(\alpha\beta)^2=\iota \tag{7.51}$$

给定的 $2n$ 阶的二面体群.

我们记得这群曾在第二章习题 7 中提到过.

对于二面体群的运算找出解析表示是有趣的. 设 x 是一取值为整数1,2,···,n的变量,1,2,···,n 表示薄片按照反时钟方向次序的顶点.运算 α 用同余关系描写为

$$x\alpha \equiv x+1(\bmod n). \qquad (7.52)$$

假如我们写 $x=1+z$, 那么 x 在 β 下的象是 $1-z$. 因而

$$x\beta \equiv 2-x(\bmod n). \qquad (7.53)$$

生成元 α 与 β 之间的所有关系可以从(7.52)与(7.53)导出. 例如,我们有

$$x\alpha\beta \equiv (x+1)\beta \equiv 2-(x+1) \equiv 1-x,$$
$$x(\alpha\beta)^2 \equiv (1-x)\alpha\beta \equiv 1-(1-x) \equiv x.$$

它断定$(\alpha\beta)^2=\iota$.

(ii) 四面体群. 绕中心 O 自由旋转的正四面体的对称群称为四面体群,共有 12 种旋转能使四面体与本身重合. 首先我们选择四种运算, 它将顶点 1 带到任一顶点 1,2,3,4 的位置, 然后假如 1 占有 x 位置, 立体可以绕直线 Ox 旋转角度 $0, 2\pi/3$ 或 $4\pi/3$,凭借这一旋转, 相交于 x 的三个面循环地交换, 因而我们一共有 $4\times3=12$ 个运算.

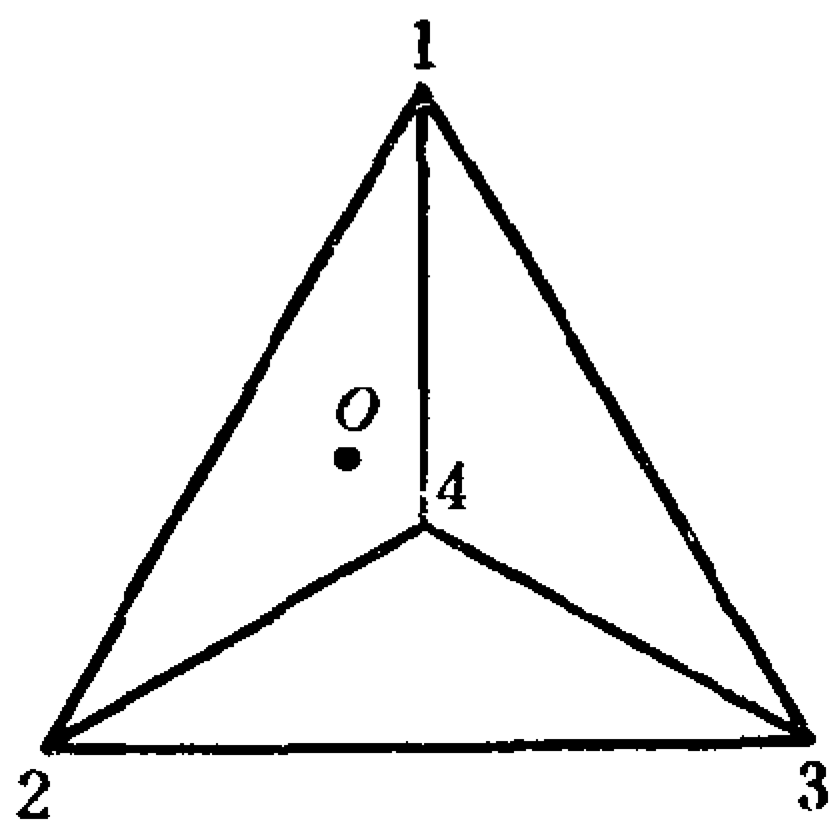


图 4

四面体群的运算用某些方法交换了四个顶点,因此这群与 S_4 的子群同构,当一顶点固定,其余三个顶点, 比如说,a,b,c 可以循环地交换, 因而四面体群包含所有(abc) 形式的轮换. 由命题 27, 这些轮换生成交代群 A_4. 因为这两个群都是 12 阶, 所以我们已经证明四面体群与 A_4 同构.

(iii) **八面体(六面体)群.** 正八面体各面的中心可以看作一立方体(六面体)的顶点. 反之,对每一立方体我们可以内接一八面体,它的顶点位于立方体各面的中心. 因而这两个体具有同样的对称, 即假如其中一个变换到它本身, 另一个也这样. 所以, 八面体群与六面体群是等同的, 虽然通常只用前一个名称. 在目前的讨论中我们觉得考虑立方体的对称比考虑八面体的对称更方便.

我们注意到立方体群由 24 种运算组成. 因为, 首先,给定的某一顶点可以变到八个顶点中任一个顶点的位置. 然后,立体可以绕通过这顶点的直径旋转 0, $2\pi/3$或 $4\pi/3$ 角度, 总共给出 $8\times 3=24$ 种旋转,包括恒等旋转在内.

立方体有四根直径 (通过中心O联结一对相对的顶点的直线). 当立方体变换到它本身, 这四根直径按某种方式交换,因而立方体群同态地映射到 S_4 中. 其次,我们决定这一同态的核. 假如某一特殊直径变到它本身上, 那么, 或者这根直径与旋转轴重合,或者直径的两个端点互相交换;在后一种情况中旋转轴垂直于这根直径,旋转角大小是 π. 属于核的旋转将使四根直径变到它自身,因此旋转轴至少必须垂直于其中三根直径. 显然,这是不可能的,除非运算是恒等运算,因而核是平凡的. 于是八面体群与S_4同构.

(iv) 二十面体(十二面体)群. 现在转向最后两个正多面体. 我们注意到二十面体和十二面体具有相同的对称. 因为二十面体的二十个面的中心可以联结形成正十二面体;反之,正十二面体十二个面的中心可以看作二十面体的顶点. 因而二十面体群与十二面体群是等同的. 两个立体都可以用来考察这群的结构,我们决定选择十二面体.

首先,我们注意十二面体群包含 60 个运算. 因为任一顶点可以变到二十个顶点中的任一个顶点的位置,然后,立体可以围绕通

过这顶点的直径旋转.这运算引起三个面的循环交换,这三个面相交于这直径的端点,因而可能的旋转角是 0, $2\pi/3$ 或 $4\pi/3$. 因此得出总共有 $20\times3=60$ 个运算, 包括恒等变换在内,这 60 个运算都使十二面体群与本身重合.

其次,我们寻求十二面体群的忠实置换表示. 结果是这群与 S_5的某一子群同构.因而我们将要描写五个对象,当十二面体旋转到与本身重合时,它们彼此交换. 根据欧几里得的古典作图法*,立方体可内接于十二面体内,

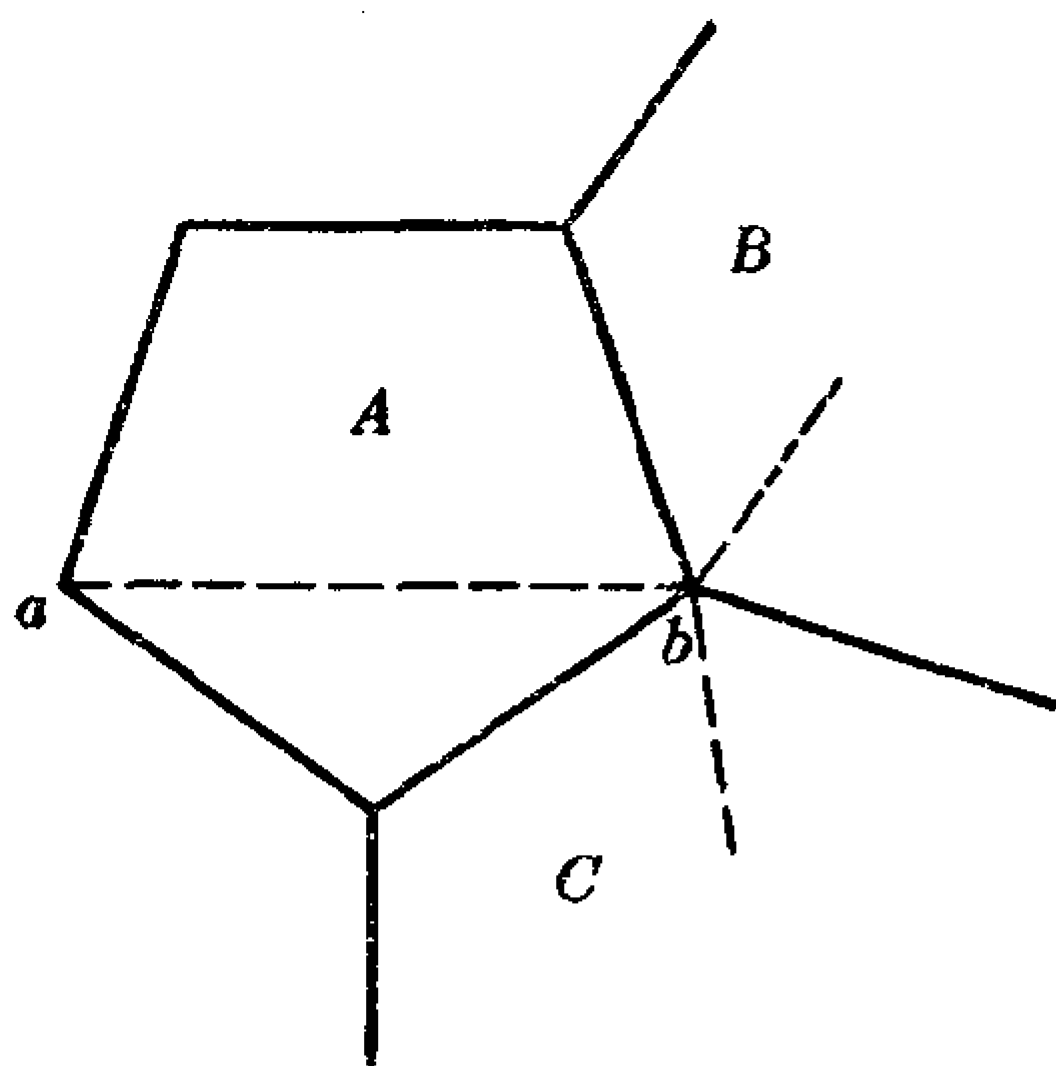


图 5

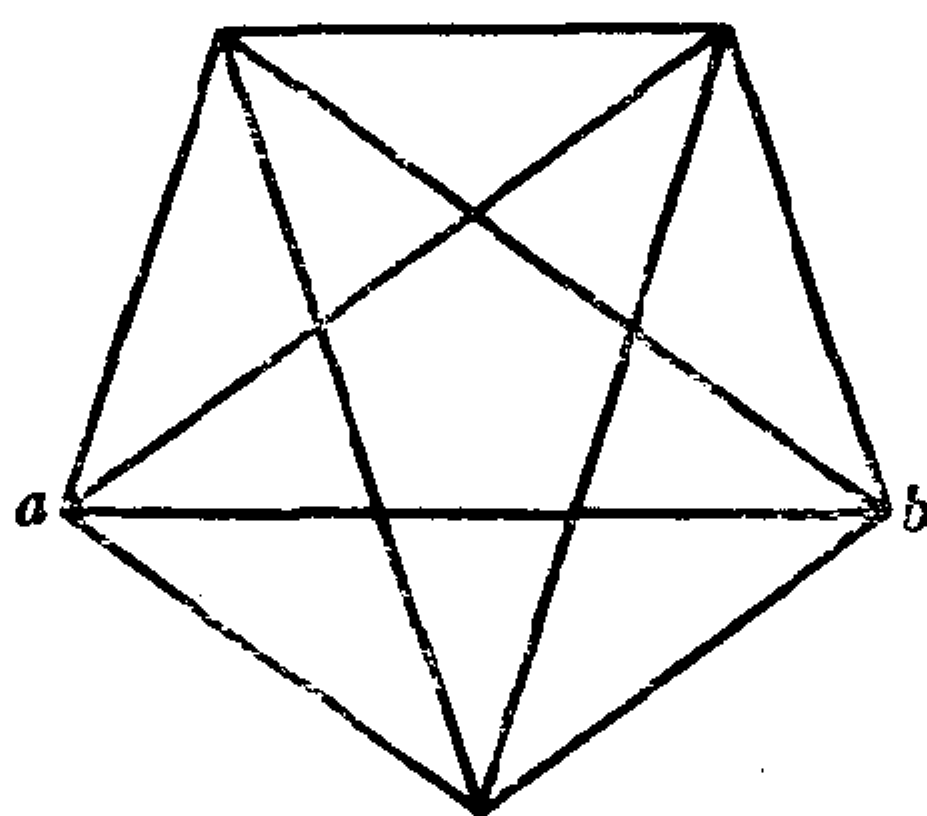


图 6

作法如下:选择某一面 A 在 A 上画一对角线, 比如说 ab,(对角线是联结面上两个不相邻顶点的直线). 在 b 点, A 面与另外两个面相邻,比如说, B 与 C. 于是我们可以证明在 B 中和在 C 中都只有一根对角线与 ab 垂直,这些新的对角线也彼此互相垂直. 于是对于 B 和 C 上的对角线再重复以上的作图法, 在这两根对角线的另一端点我们在相邻的两面中确定另外两根对角线, 它们与原来的对角线一起共同形成直三面角,等等. (以上所说的最好用观察模型来证实.)因此从 ab 开始,我们在十二个面中的每一面内挑选出

* *Elements*, Book XIII. 命题 17.

唯一的对角线，这些对角线形成内接于十二面体的立方体的边．因为每一面有5根对角线(图6)，而我们可以从其中任一根对角线开始按上述方法作图，因而可作五个立方体内接于十二面体，而这些立方体在十二面体上的任一对称运算中互相交换．因此我们已经找到五次的置换表示．此外，这表示是忠实的，即将每一个立方体重合于本身的任一旋转必然是恒等变换．(我们要求读者接受这一事实而不给予进一步的证明．)因此十二面体群与S_5的某一子群同构，因为它的指数是2，它一定是正规子群(§19末尾的(iv))，从而我们由命题28断定，二十面体(十二面体)群与A_5同构．

习　题

(1) 证明 $(ab\cdots lx)(x\alpha\beta\cdots\lambda)=(ab\cdots l\alpha\beta\cdots\lambda x)$，此处 $a,b,\cdots,l,x,\alpha,\beta,\cdots,\lambda$ 是不同的符号．

(2) 由 r 个彼此不相交的轮换(包括1阶的轮换)的积所形成的 n 次置换是偶置换或奇置换，根据 $n-r$ 是偶数或奇数而定．

(3) 证明 S_n 可以由下列对换生成

$$(12),(23),\cdots,(n-1\ n).$$

(4) 证明 S_n 可以由下列置换生成

$$\gamma=(12\cdots n)\quad 及\quad \tau=(12).$$

(5) 证明正则置换可以表示成轮换的幂．反之，假如 $\gamma=(12\cdots m)$，那么 γ^s 是由 d 个 r 次的轮换组成的正则置换，此处 $d=(m,s)$ 及 $r=m/d$．

(6) 证明 $\gamma=(a_1a_2\cdots a_n)$ 在 S_n 中的中心化子由 $\iota,\gamma,\gamma^2,\cdots,\gamma^{n-1}$ 组成．

(7) 证明当 $n>2$，$\lambda=(a_1a_2\cdots a_{n-1})$ 在 S_n 中的中心化子由 $\iota,\lambda,\lambda^2,\cdots,\lambda^{n-2}$ 组成．

(8) 证明当 $n>2$，S_n 的中心仅由恒等变换组成．

(9) 群 G 的**左正则表示**的定义是：对应 G 的某一固定元素 u，存在置换 λ_u，它按规则 $a\lambda_u=u^{-1}a$ 作用在 G 的元素上 $(a\in G)$．证明(i) $\lambda_u\lambda_v=\lambda_{uv}$ (ii) $\lambda_u=\iota$，当且仅当 $u=1$；(iii) $\lambda_u\rho_x=\rho_x\lambda_u$，此处 ρ_x 由(7.42)定义；(iv)假如

是 G 中元素的置换，它与所有的 λ_u 交换，那么对于某一 x，$\theta=\rho_x$，以及假如 η 与所有 ρ_x 交换，那么对于某一 u，$\eta=\lambda_u$。

(10) 证明：假如 G 是阶为 168 的单群，H 是 G 的真子群，那么 $[G:H]\geqslant 6$。

(11) 求出矩形(非正方形)薄片的对称群。

(12) 证明：当 n 次可迁群的 g 个元素写成次数大于 1 的彼此不相交的轮换的积时，那么它们包含 $(n-1)g$ 个文字。

第八章　西洛(Sylow)定理

§ **46. 素数幂子群.** 拉格朗日定理说明，假如G是g阶的有限群，那么G的子群的阶一定能整除g. 可是这定理的逆定理不成立；因为我们已经知道存在这样的g阶群(§ 42 最后一个例题)，它不包含阶为g的某一因子的子群. 可是，假如p^b是素数p的幂，使得p^b整除g，那么G至少具有一个p^b阶的子群. 这件值得注意的事实在1872年被挪威数学家L.西洛(L.Sylow)所发现. 在群论中这件事具有深远的影响，它提供了在群的算术性质和结构性质之间的精巧联系的最突出的例子之一. 西洛的著名结论的几个证明可以在文献中找到. 这里我们介绍*一个属于H.威兰(H.Wielandt)的优美的证明；这证明从最初等的原理出发，只利用置换的某些初等概念.

定理 27　设G是g阶有限群. 又设p是素数使得p^b整除g. 此处b是正整数，那么G具有m个p^b阶的子群，此处m是满足$m \equiv 1 \pmod{p}$的正整数.

证明 (1)写出

$$g = p^b z, \tag{8.1}$$

此处z是正整数，它不需要与p互素，列出所有G的p^b个不同元素组成的子集，设为$\mathscr{K}$. 因而假如有n个这样的子集，我们写成

$$\mathscr{K}: \ K_1, K_2, \cdots, K_n. \tag{8.2}$$

事实上，n等于二项式系数$\binom{g}{p^b}$，不过以后并不需要这知识. 本定理肯定子集(8.2)中至少有一个是子群.

利用§ 8 关于基数的记号，子集K属于$\mathscr{K}$当且仅当

---

* 我们的证明仿效B.Huppert, *Endliche Gruppen* I (Springer, 1967) p.33.

$$|K|=p^b.$$

假如x是G的任一元素，那么$|Kx|=|K|$，因而Kx也属于$\mathscr{K}$. 事实上，映射

$$K_i \to K_i x \qquad (i=1,2,3,\cdots,n)$$

构成$\mathscr{K}$的一个置换. 在这个意义上，我们说G作用在$\mathscr{K}$上. 关于这作用，我们可以如下规定$\mathscr{K}$上的一个等价关系：子集K_i与K_j称为等价的，假如存在G的元素x，使得$K_i=K_j x$. 读者不难证实这规定满足通常的等价关系公理. 结果，$\mathscr{K}$分成互不相交的等价类或象在这里所称的轨道. 因而K的轨道，我们将以$o(K)$表示，由所有形状为$Kx(x\in G)$的子集组成. 当x遍历G时，我们一般会几次得到轨道的每一元素，包含在$o(K)$中不同子集的个数可写为$|o(K)|$. $\mathscr{K}$按轨道的分解式可表示如下：

$$\mathscr{K}=o(K)\cup o(K')\cup o(K'')\cup\cdots, \tag{8.3}$$

此处$K, K', K'', \cdots$是一组轨道的代表. 计算两边元素的个数，我们得出

$$n=|o(K)|+|o(K')|+|o(K'')|+\cdots. \tag{8.4}$$

(2)我们接着更详细地考查某一轨道，比如说$o(K)$. 设S是K在G的作用下的稳定化子，即

$$S=\{u\in G\,|\,Ku=K\}.$$

读者易于证实S是G的子群. 假设

$$G=\bigcup_{i=1}^{r} St_i \quad (t_1=1)$$

是G对于S的右陪集分解式. 我们断定$o(K)$由子集

$$Kt_1, Kt_2, \cdots, Kt_r \tag{8.5}$$

组成. 显然，所有这些子集属于$o(K)$，而且它们彼此不同. 因为假如$Kt_i=Kt_j$，那么$Kt_it_j^{-1}=K$，即$t_it_j^{-1}\in S$，因此$St_i=St_j$，这意味$i=j$. 其次，$o(K)$中任一项的形状是Kx，假设x位于陪集St_i内，我们有$x=ut_i$，此处$u\in S$，所以$Kx=Kut_i=Kt_i$. 因而我们已经

证明

$$|o(K)|=[G:S]. \tag{8.6}$$

关于S的进一步的结果可以从K具有素数幂基数中得到. 稳定化子的定义性质作为G的子集间的关系，可用以下方程表示：

$$KS=K.$$

更精确地说，假如$K=v_1\cup v_2\cup v_3\cdots$，我们有

$$K=v_1S\cup v_2S\cup v_3S\cup\cdots. \tag{8.7}$$

因而K是S的左陪集的并集. 我们知道两个这样的陪集或者不相交或者全同，以及每一个陪集包含$|S|$个元素. 因而假如(8.7)中不同陪集的个数等于f，我们有

$$p^b=f|S|.$$

那么$|S|$是p的某次幂，比如说

$$|S|=p^c, \tag{8.8}$$

此处$c\leqslant b$. 现在必须区别两种情况.

(i) $|S|=p^b$. 我们还不知道是否这种情况会发生. 假如发生的话，那么

$$|o(K)|=g/p^b=z,$$

此处z在(8.1)中下过定义. 既然$|S|$现在取最大的值，我们可以称$o(K)$为**最小轨道**. 因为由目前的假设K与S具有相同基数，我们从(8.7)肯定K退化到一个陪集，比如说

$$K=vS \quad (v\in K).$$

子集

$$H=Kv^{-1}=vSv^{-1}$$

显然属于$o(K)$，并且是子群，即与S共轭的群. 因而我们得出结论：每一最小轨道至少包含一子群. 因为$|H|=p^b$，那么

$$[G:H]=z=|o(K)|.$$

设

$$Hw_1, Hw_2, \cdots, Hw_z \tag{8.9}$$

是H在G中的陪集. 这z个都属于$o(K)$，因为H属于$o(K)$. 又因

为它们彼此不相同，所以它们构成全部$o(K)$. 但是我们知道只有一个陪集，即H，是子群. 因而我们已经证明最小轨道包含一个也仅仅包含一个G的子群.

(ii) $|S|=p^c<p^b$，在这情况轨道$o(K)$不是最小，而

$$|o(K)|=g/p^c=zp^{b-c},$$

因而

$$|o(K)|\equiv 0(\mathrm{mod}\,pz). \tag{8.10}$$

非最小轨道不能含有子群. 因为假如它含有，我们可以选择这个群作为$o(K)$的生成元，因而不失普遍性，假定K本身是群. 那么K将位于它自己的稳定化子中，因为$KK=K$(见(2.6)式). 因而$|S|\geqslant|K|=p^b$，这与假设(ii)是不相容的.

(3)回到(8.4)，我们把最小项，假如有的话，从其他项中分出. 每一最小轨道恰好具有一个子群，而不同的最小轨道含有不同的子群，因为轨道不相交. 对于每一最小轨道，基数$|o(K)|$等于z，这样的最小轨道个数等于本定理中所规定的整数m.(可是注意，这时我们仍旧不知道m是否是正的.)因而所有最小轨道对(8.4)的全部贡献等于mz. 因为由(8.10)可知(8.4)中其余的每一项都可被pz整除，所以我们可以用下面的同余总结这情况

$$n\equiv mz(\mathrm{mod}\,pz). \tag{8.11}$$

下面的性质是证明的关键. 即我们在本证明一开始所定义的数n只依赖G的阶，而不依赖它的构造. 因而对于所有p^bz阶的群，n具有相同的数值，可是对于固定的n，m各不相同. 因此我们应该将(8.11)更明显地写成

$$n=m_Gz+K_Gpz,$$

此处m_G与K_G是依赖G的整数. 为了得到关于n的信息，我们应用这结果到p^bz阶的循环群C上. 从定理4 (§ 11) 我们知道C恰好只具有一个p^b阶的子群. 因而$m_C=1$，所以

$$n=z+K_Cpz.$$

将n的两个表示式相等起来，我们得出

$$z+K_C pz=m_G z+K_G pz,$$

通除以z从而

$$m_G\equiv 1(\mathrm{mod}\, p),$$

象所要求的那样.

§ 47. 西洛(Sylow)定理. 通常用三个定理介绍西洛得出的结果. 本节我们将要给出这三个定理.

定理 28（西洛第一定理） 假如p^a是能整除群G的阶的素数p的最高次幂. 那么，G至少具有一个p^a阶的子群.

证明 这是定理 27 的特殊情况，它对应指数 b 的最大可能的数值.

定义 14 令G是g阶有限群。假设$g=p^a g'$，此处p是素数且$(g',p)=1$. 那么，任一G的p^a阶的子群称为G的**西洛p-群**.

群G对应于同一素数可以具有不止一个西洛群. 事实上，假如P是p^a阶子群，$x^{-1}Px$也是p^a阶子群，此处x是G的任一元素. 换句话说，西洛群的共轭群也是西洛群. 当然，共轭群不需要彼此不相同. 但是下面的定理告诉我们不能存在另外的西洛群.

定理 29（西洛第二定理） G的所有属于同一素数的西洛群在G中彼此共轭.

证明 象在定义 14 中那样，令$|G|=g=p^a g'$，此处$(g',p)=1$. 假设A与B是p^a阶子群，我们利用G对于A与B的双陪集分解(§ **16**，定理 6)，因而在目前情况中，

$$G=At_1B\cup At_2B\cup\cdots\cup At_rB,$$

$$g=p^{2a}\sum_{i=1}^{r}d_i^{-1}, \tag{8.12}$$

$$d_i=|t_i^{-1}At_i\cap B|. \tag{8.13}$$

将(8.12)两边除以p^a我们得到

$$g'=p^a\sum_{i=1}^{r}d_i^{-1}. \tag{8.14}$$

因为 d_i 是 B 的子群的阶,因而必须等于 p 的非负幂. 因而(8.14)右边每一项或者等于1,或者是 p 的具有正指数的幂. 但是 g' 不可以被 p 整除,因此右边必须至少有一项等于1, 比如说 $p^a d_j^{-1}=1$,即 $d_j=p^a$.于是我们有

$$p^a=|t_j^{-1}At_j\cap B|.$$

既然群 $t_j^{-1}At_j$ 与 B 都是 p^a 阶,它们的交集只有当它们等同时才能够是 p^a 阶. 因而

$$B=t_j^{-1}At_j,$$

即 A 与 B 是共轭的,象本定理所断定的那样.

推论 1 *有限群 G 对于给定的素数 p 具有唯一的西洛群 P,当且仅当 P 在 G 中是正规的.*

证明 唯一性条件等于说对于 G 中所有 x,$x^{-1}Px=P$,但是这意味 P 是正规子群.

在有限阿贝尔群的情况中,西洛群必然是唯一的. 西洛群的概念与 p-准素分支(§28)的概念是一致的.在乘法术语中定理16(§28)可以重新阐述如下.

推论 2 *有限阿贝尔群是它的西洛群的直积.*

下面的定理更精确地给出关于西洛群个数的结果.

定理 30 **(西洛第三定理)** *设 r 是 G 的西洛 p-群的个数. 那么 r 是形为 $1+pk$ 的整数,且是 G 的阶的因子.*

证明 $r\equiv 1 \pmod p$ 已经在定理27中证明过了. 还需证明 $r|g$,此处 $g=|G|$. 令

$$\mathscr{P}:\ P_1(=P),P_2,\cdots,P_r$$

是所有 G 的西洛 p-群的集合,那么,由定理29,$\mathscr{P}$ 是全部 P 的共轭群组. 已经做过第三章习题6的读者会知道

$$r=[G:N(P)], \tag{8.15}$$

此处 $N(P)$是P在G中的正规化子. 因而,假如$|N(P)|=n$, 那么 $g=nr$,这证明了 $r|g$. 关系式(8.15)类似(8.6).事实上,我们可以定义G在$\mathscr{P}$集上的作用为联系G的任一元素 x 的映射

$$P\to x^{-1}Px(P\in\mathscr{P}),$$

它导致一个 $\mathscr{P}$ 的置换. 当 x 遍历G时,可以得到 $\mathscr{P}$的任一元素,即全部 $\mathscr{P}$ 是P的轨道,而我们有

$$|o(P)|=r.$$

P的稳定化子由G的那些元素组成,对于它们$u^{-1}Pu=P$. 因而在目前所讨论的这种情况中, P 的 稳 定 化 子变成正规化子. 用 $N(P)$代替S,(8.6)就化成(8.15).

§ 48. 应用与例. 对于考查有限群的结构,西洛定理提供了有力的工具. 当这群对某一素数具有唯一的西洛群时,这方法特别有效.

命题 31 *当G是 pq 阶群,此处 p 与 q 是素数,使得 $p<q$, 及 $q\not\equiv 1\ (\mathrm{mod}\ p)$. 那么$G$一定是阿贝尔群.*

证明 令 r 是西洛 p-群的个数. 由 定 理 30, $r|pq$, $r=1+pk$. 显然,$(r,p)=1$ 因而 $r|q$. 因为 q 是素数,那么或者 $r=1$ 或者 $r=q$. 后面一种情况意味 $q=1+pk$ 即 $q\equiv 1(\mathrm{mod}\ p)$, 根 据本定理的假设我们已经排除了这种情况. 因而由 推 论 1,G只具有一个 p 阶的正规子群,它必须是循环的. 我们用 u 表示 它的生成元. 因而

$$P\lhd G,P=\mathrm{gp}\{u\}. \tag{8.16}$$

其次,假设G具有 s 个西洛 q-群,那么 $s|pq$,而且 $s=1+ql$. 因为$(s,q)=1$,我们必然有 $s|p$,因而 $s<p$. 假如 $l\geqslant 1$, 那么 $s\geqslant 1+q>p$,这是一个矛盾. 因此 $l=0$,而G具有一个 q 阶正 规子群 Q,它具有生成元 v,因而

$$Q\lhd G,Q=\mathrm{gp}\{v\}. \tag{8.17}$$

因为P与Q的阶互素，

$$P\cap Q=\{1\}. \tag{8.18}$$

于是由命题 11(§ 23)，P与Q的元素成对地交换. 特别

$$uv=vu. \tag{8.19}$$

积

$$u^{\alpha}v^{\beta}(\alpha=0,1,\cdots,p-1;\beta=0,1,\cdots,q-1)$$

是不同的，因为它们之间的等式将与(8.18)矛盾. 因而这些元素构成整个群，而(8.19)表明这群是阿贝尔群.

例 1 不可能有 200 阶的单群.

因为既然 $200=5^2\times 8$，这群包含r个 25 阶的西洛群，此处r的形式是$1+5k$，r又是 200 的因子. 因为$(r,5)=1$，我们必有$r|8$，这是不可能的，除非$k=0$. 因而这群含有唯一的 25 阶正规子群. 因此不是单群.

例 2 不可能有 30 阶的单群.

因为假如有这样的单群，那么它的西洛群都不是唯一的. 因而将有$1+5(=6)$个不同的 5 阶的西洛群，共包含$6\times 4(=24)$个 5 阶元素. 类似地，将有$1+3\times 3(=10)$个不同的 3 阶西洛群，共包含 20 个 3 阶的元素. 因而元素的数目将超过 30.

我们继续讨论一个关于西洛群的更一般的结论.

定理 31 设P是有限群G的西洛子群，又假设H是G的子群，H包含P的正规化子，那么H是它自己的正规化子.

证明 令$u\in N(H)$，$N(H)$是H的正规化子，即$u^{-1}Hu=H$. 因为$P\leqslant N(P)\leqslant H$，所以$u^{-1}Pu\leqslant u^{-1}Hu=H$，因而与$P$同阶的$u^{-1}Pu$也是$H$的西洛群. 对$H$应用定理 29，我们断定存在$H$的元素$h_1$使得

$$h_1^{-1}(u^{-1}Pu)h_1=P.$$

这意味uh_1属于$N(P)$. 因为，根据假设$N(P)\leqslant H$，所以$uh_1=h_2$，此处$h_2\in H$. 因而$u\in H$，这就证明了定理. 最后，我们要指

出在§47推论2中提到的性质实际上是所有有限幂零群的特征.

定理 52 令G是$p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$阶有限群，$P_1, P_2\cdots, P_r$是一组$G$的西洛群分别对应于素数$p_1, p_2, \cdots, p_r$. 那么$G$是幂零群当且仅当

$$\text{(i)}\ P_i \lhd G(i=1,2,\cdots,r),\text{及}$$

$$\text{(ii)}\ G=P_1\times P_2\times\cdots\times P_r. \tag{8.20}$$

证明 首先，假设(8.20)成立，我们知道直积中的每一因子是正规子群(§13). 还由§38例2，知道每一西洛群是幂零群. 尚需证明幂零群的直积也是幂零群. 于是假设K与L是幂零群，考虑群$K\times L$. 假如$\Gamma_i(K)$, $\Gamma_i(L)$, $\Gamma_i(K\times L)$分别是对于K, L及$K\times L$的序列(6.18)的典型项，那么，显然

$$\Gamma_i(K\times L)=\Gamma_i(K)\times\Gamma_i(L)\quad(i=1,2,\cdots).$$

因而假如$\Gamma_i(K)$与$\Gamma_i(L)$对于足够大的i值退化到单位元群，那么$\Gamma_i(K\times L)$也退化到单位元群，即$K\times L$是幂零群. 因此(8.20)意味G的幂零性.

反之，假设G是有限幂零群，设P是G对于某一特殊素数的西洛群. 令$H=N(P)$. 我们断定$H=G$，即$P\lhd G$. 因为假如$H<G$，即H是真子群，那么由§38命题20，$N(H)>H$；另一方面，由定理31，$N(H)=H$. 这个矛盾证明$H=G$. 因而$P_i\lhd G(i=1,2\cdots,r)$.

显然，$P_i\cap P_j=\{1\}$当$i\neq j$. 因而由§13命题11及内直积(§13)的定义，

$$P_1P_2\cdots P_r=P_1\times P_2\times\cdots\times P_r.$$

这是阶为$p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$的子群，因此与$G$重合.

习 题

(1) 证明A_4有一个4阶西洛群和四个3阶西洛群.

(2) 求出一个S_4的西洛2-群。它与§14所给出的群中哪一个同构? 共

有多少西洛 2-群？

(3) 证明不存在 56 阶的单群。

(4) 假定 G 是 p^2q 阶的群，此处 p 与 q 是素数使得 q 小于 p，同时 q 也不是 p^2-1 的因子。证明 G 是阿贝尔群。

(5) 设 p 是能整除群 G 的阶的素数。证明假如 K 是 G 的子群，使得 $|K|$ 是 p 的幂，那么 K 至少包含在一个西洛 p-群内。

(6) 证明正规 p-子群包含在每一个西洛 p-子群中。

(7) 设 P 是有限群 G 的西洛 p-群，又设 H 是 G 的正规子群。证明 (i) HP/H 是 G/H 的西洛 p-子群，(ii) $H\cap P$ 是 H 的西洛 p-子群。

习 题 解 答

第 一 章

(2) 结合律不适用.

(3) $xa^n=a^nx+\beta(a^n-1)/(a-1)$.

(4) $ab=(ab)^{-1}=b^{-1}a^{-1}=ba$.

(5) $ba=a^{-1}(ab)a$,见§5关于群的元素的阶的事实(iii).

(6) 注意 $a^mb^{n-2}=b(ab^{-1})b^{-1}, a^{m-2}b^n=a^{-1}(a^{-1}b)a$.

(8) 存在整数 u,v 使得 $um+vn=1$;令 $y=x^{vn}, z=x^{um}$.

(9) 不满足方程 $x^2=1$ 的元素可以分成许多不相交对 $(u,u^{-1}),(v,v^{-1})$, $\cdots$,因此方程具有偶数个解,其中一个是1.

(10) 这些阶分别是1,3,6,3,6,2,并且3或5可以用作生成元.

(13) (i) (1478)(265)(39);(ii) $(acdf)(be)$.

(14) (i) $(ab\cdots kl)$;(ii) $(a_ryb_1\cdots b_sxc_1\cdots c_t)$;

(iii) $(a_ryc_1c_2\cdots c_t)(xzb_1b_2\cdots b_s)$.

第 二 章

(2) 假如 $u,v\in At\cap Bs$,那么 $uv^{-1}\in A\cap B$,因此 $Du=Dv$. D 的不同陪集的个数不能超过非空交集 $At\cap Bs$ 的个数,G 的每一元素必位于这些交集之一中.

(3) 因为 $|A\cap B|$ 能整除 $|A|$ 和 $|B|$,所以 $|A\cap B|=1$.

(4) 假如 G 是循环群,由定理4可得此结果. 假如 G 不是循环群,设 $x\in G$ 及 $x\neq1$;那么 $\mathrm{gp}\{x\}$ 是一真子群.

(5) $\mathrm{gp}\{a\},\mathrm{gp}\{a^2,b\},\mathrm{gp}\{ab,a^3b\}$.

(6) 只要证明这些关系式蕴含§14中给出的 $G=\mathrm{gp}\{a,c\}$ 所服从的关系式就够了. 于是由 $a=cd, ac=cdc$,从而 $a^3=1,(ac)^2=1$.

(9) 将元素写成以下形式,$a^k, a^kb(0\leqslant k\leqslant5)$, $c=b^{-1}ab$ 一定是 a 的幂,

且与 a 有相同的阶。又因为 $c=a$ 被排除，所以一定有 $c=a^{-1}$。还有，对于适当的 l，$b^2=a^l$，因而 $b^2=b^{-1}b^2b=b^{-1}a^lb=a^{-l}$。因此 $a^{2l}=1$，从而 $l=0$ 或 $l=3$。

(10) 例如，gp$\{2\}\times$gp$\{-1\}$，即 gp$\{2\}\times$gp$\{20\}$。

第 三 章

(1) 假如 $b=t^{-1}at$，那么 $a^m=1$ 意味 $b^m=1$，反过来也是正确的。

(2) (i) 假如 $C(a)$ 是 a 的中心化子，那么 $C(a)=C(a^{-1})$，从而由命题 7 得出结论。(ii) 利用类方程(3.5)，此处可设 $h_1=1$；假如结论是错误的，余下的项可以分成一对对相等的项，每一对相等的项对应一互逆类。但是这样 g 将是奇数与假设矛盾。

(3) 设 $\boldsymbol{a}=(a_{ij})\in Z$，$Z$ 是 G 的中心。那么对于所有的 $x\in G$，$\boldsymbol{ax}=\boldsymbol{xa}$。特别我们可以取 $\boldsymbol{x}=\mathrm{diag}(x_1,x_2,\cdots,x_n)$，为一具有不同的对角线元素的对角矩阵。那么 $a_{ij}x_j=x_ia_{ij}$，从而 $a_{ij}=0$ 当 $i\neq j$ 时；因而 $\boldsymbol{a}$ 本身是一对角矩阵。其次，取 $\boldsymbol{x}$ 为置换矩阵 $\boldsymbol{p}=(p_{ij})$，此处 $p_{i,i+1}=1(i<n)$，$p_{n,1}=1$，而其他 $p_{i,j}=0$。方程 $\boldsymbol{ap}=\boldsymbol{pa}$ 意味 $a_{11}=a_{22}=\cdots=a_{nn}$，即 $\boldsymbol{a}$ 是纯量矩阵。

(4) $Z=$gp$\{a^2\}$。G/Z 的元素是 Z,Za,Zb,Zab，$G/Z\cong V$(见 §14)。

(5) 假如 $\boldsymbol{s}$ 与 $\boldsymbol{t}$ 是上三角矩阵，那么 $\boldsymbol{st}$ 是具有对角项 $s_{11}t_{11},s_{22}t_{22},\cdots,s_{nn}t_{nn}$ 的上三角矩阵，从而易于证明 T 具有群的性质。设 $\theta:T\to D$ 是由 $\boldsymbol{t}\theta=\mathrm{diag}(t_{11},t_{22},\cdots,t_{nn})$ 定义的映射。那么 E 是 θ 的核，由第一同构定理得出本题结论。

(6) 注意 $x^{-1}Hx=y^{-1}Hy$ 当且仅当 $xy^{-1}\in N(H)$，即 $N(H)x=N(H)y$。(见命题 7 的证明)。

(7) G/N 是 n 阶的有限群，G/N 的元素 Nt 是 h 阶的。因而，由于拉格朗日定理，$h|n$。还有 $(Nt)^r=Nt^r=N$，从而 $h|r$。(见 §5，命题 1)。

(8) 两部分都可用关于 k 的归纳法证明。利用 $ab=bac,ac=ca$ 及 $bc=cb$。

(9) 由第三同构定理，$A/A\cap N\cong NA/N$，NA/N 是 n 阶有限群 G/N 的子群。因而 $|A/A\cap N|$ 能整除 n。

(10) 在这些群中的每一个中，中心都是 $Z=$gp$\{a^2\}$。因为 $a^2=[a,b]$，所以 $a^2\in G'$，因而 $Z\leqslant G'$。另一方面，G/Z 是 4 阶的因而是阿贝尔群。因此

(由定理 11),$G'\leqslant Z$,从而$G'=Z=\mathrm{gp}\{a^2\}$。

(11) 设$N\lhd G$及$C=C(N)$。因而假如$c\in C$,那么对于所有的$u\in N$,$cu=uc$。假如$t\in G$,那么$c^tu^t=u^tc^t$;但是u^t可以等于N的任一元素,因而$c^t\in C$,所以$C\lhd G$。

(12) $(xy)\theta=(xy)^{-1}=y^{-1}x^{-1}=x^{-1}y^{-1}=(x\theta)(y\theta)$。 易于证明$\theta$是双射。

(13) 设$x\tau=t^{-1}xt$是一内自同构,α是任一自同构;令$s=t\alpha$及$x\sigma=s^{-1}xs$。 因而 $x\alpha\sigma=s^{-1}(x\alpha)s$, $x\tau\alpha=(t^{-1}xt)\alpha=s^{-1}(x\alpha)s$。 因而$\alpha\sigma=\tau\alpha$,$\alpha^{-1}\tau\alpha\in I(G)$,$I(G)\lhd A(G)$。

(14) 设$\alpha\in A(G)$;那么$[a,b]\alpha=[a\alpha,b\alpha]\in G'$。因而$G'\alpha\subset G'$。 相似地,$G'\alpha^{-1}\subset G'$。因而$G'\subset G'\alpha$,从而$G'\alpha=G'$。

第 四 章

(1) 构造自由阿贝尔群$F=\langle u_1,u_2,\cdots,u_n\rangle$,令$v_1=b_1u_1+b_2u_2+\cdots+b_nu_n$。存在元素$v_2,v_3,\cdots,v_n$使得$F=\langle v_1,v_2,\cdots,v_n\rangle$及$v_i=\sum_j b_{ij}u_j$,此处$(b_{ij})$是具有所要求的性质的幺模矩阵。

(2) 令$|A|=p_1p_2\cdots p_n$。在(4.47)中准素分支P_i是p_i阶的,因而是循环群,比如说$P_i=\mathrm{gp}\{x_i\}$。 于是$x=x_1+x_2+\cdots+x_n$是$p_1p_2\cdots p_n$阶的元素,因而生成A。

(3) 设e_1是最大不变量。t_ρ不出现在(4.37)中,w_1是e_1阶的,而每一元素满足$e_1x=0$。

(4) $\phi(24)(=8)$个剩余类中的每一个满足$x^2\equiv1(\mathrm{mod}\ 24)$。

(5) (i) 4,3,5;60。(ii) (4,2),3,(5,5);60,10。

(6) $C_\infty\oplus C_3\oplus C_6$。

(7) (i) $r=1,e_1=2$;(ii) $r=2,e_1=2$。

(8) $v_1=u_1+u_2+ku_3,u_2=u_2-u_3,v_3=-u_3;s_1=r_3,s_2=r_2-r_3,s_3=r_1+r_2-(k+1)r_3$。 $e_1=1,e_2=k-1,e_3=(k-1)(k+2)$。

(9) 由于定理 16, 所以只要对一个素数幂阶的阿贝尔群P证明命题就够了。设$|P|=p^m$。我们必须证明,假如$n\leqslant m$,则存在子群P'使得$|P'|=$

p^n. 假设 $P=\sum_i \oplus P_i$，此处 $|P_i|=p^{\delta_i}$. 那么 $m=\sum_i \delta_i$. 显然，我们能写成 $n=\sum_i \lambda_i$ 此处 $0\leqslant\lambda_i\leqslant\delta_i$. 由定理 4，存在 p^{λ_i} 阶子群 $P'_i\subset P_i$. 令 $P'=\sum_i P'_i$.

(11) 令这群的元素与 p^3 个向量 $\boldsymbol{a}=(\alpha_1,\alpha_2,\alpha_3)$ 等同，此处 $0\leqslant\alpha_i<p(i=1,2,3)$. 第一基向量 $\boldsymbol{a}_1$ 可以是 p^3-1 个非零向量中任一个. 第二基向量 $\boldsymbol{a}_2$ 可以是任一个不是 $\boldsymbol{a}_1$ 纯量倍的向量；共有 p^3-p 个这样的向量. 最后，$\boldsymbol{a}_3$ 使基完全，只要 $\boldsymbol{a}_3$ 不是 $\boldsymbol{a}_1$ 与 $\boldsymbol{a}_2$ 的线性组合；共有 p^3-p^2 个这样的向量. 因而我们共有 $(p^3-1)(p^3-p)(p^3-p^2)$ 种选择.

(12) 考虑自由阿贝尔群 $F=\langle u_1,u_2\cdots,u_n\rangle$ 及子群 $R=\mathrm{gp}\{r_1,r_2,\cdots,r_m\}$，此处 $r_i=\sum_j b_{ij}u_j$. 改变 F 与 R 中的生成元等于用 Q 右乘 B 及用 P 左乘 B.

第 五 章

(1) 设 F 是自由群，设 U 是这些字的集合，它们的每一生成元的指数和等于零. 那么 U 是子群，显然 $F'\subset U$. 反之，在自然映射 $F\to F/F'$ 下，U 的每一元素映射到 F' 中. 因而 $U\subset F'$，所以 $U=F'$.

(2) (i) $C_2\times C_2$，(ii) C_4.

(3) 定义关系可写成 $b^{-1}a^{-1}ba=b$，$a^{-1}b^{-1}ab=a$，从而利用相乘得出 $ab=1$. 因此 $b=a^{-1}$，于是我们得出 $a=b=1$.

第 六 章

(1) 在两种情况下，$G\rhd\mathrm{gp}\{a\}\rhd\mathrm{gp}\{a^2\}\rhd\{1\}$ 都可以作为合成列. 所有合成因子都是 2 阶的.

(2) 假设 $G^{(s)}=\{1\}$. 假如 $H\leqslant G$，那么 $H^{(i)}\leqslant G^{(i)}(i=1,2,\cdots)$. 假如 $N\lhd G$，那么 $G/N=G\nu$，此处 ν: $G\to G/N$ 是 G 到 G/N 上的自然满同态. 注意 $(G\nu)^{i}=G^{(i)}\nu(i=1,2,\cdots)$. 因而 H 与 $G\nu$ 的导出列至多在 s 步之后终止于单位元群.

(4) 因为 $\Gamma_3=[\Gamma_2G]=[G',G]=\{1\}$，$G'$ 位于 G 的中心内. 在习题(3)的公式中，$[x,z]^y=[x,z]$，$[x,y]^z=[x,y]$.

(5) 象在习题(2)中那样.

(6) 因为 $\Gamma_4=\{1\}$，$\Gamma_3=[G',G]$ 位于 G 的中心中；特别 $[v,x^{-1}]=c\in Z$

$(v\in G^1, x^{-1}\in G)$，即 $v^{-1}xv=cx$. 类似地，假如 $y\in G, v^{-1}yv=dy$，此处 $d\in Z$. 现在 $v^{-1}[x,y]v=v^{-1}(x^{-1}y^{-1}xy)v=c^{-1}d^{-1}cd[x,y]=[x,y]$，

因而 v 与 G' 的每一元素交换.

(7) 由命题 20，$M<N(M)$；因而 $N(M)=G$，即 $M\triangleleft G$. 还有 G/M 不能有真子群，因为这群将包含 M. 因此 $|G/M|$ 是一素数.

(8) $D(2^n)$ 的元素可以表示为 $a^\alpha b^\beta(\alpha=0,1,\cdots,2^n-1,\beta=0,1)$. 因为 $b^{-1}ab=a^{-1}$，中心元素必须满足 $a^\alpha b^\beta=a^{-\alpha}b^\beta$，从而 $\alpha=0$ 或 2^{n-1}，及 $\beta=0$，因为 b 不在中心内. 因而 $Z_1=\{1,a^{2^{n-1}}\}$。 假如 $\bar{a}=aZ_1$，$\bar{b}=bZ_1$，那么 $(\bar{a})^{2^{n-1}}=\bar{b}^2=(\overline{ab})^2=\bar{1}$. 上中心群列的连接的项具有指数 2.

第 七 章

(2) 设 $\xi=\sigma_1\sigma_2\cdots\sigma_r$，此处 σ_i 是 $m_i(i=1,2,\cdots,r)$ 次轮换. 因而 $n=m_1+m_2+\cdots+m_r$. 利用 (7.25)，我们得出 $\zeta(\xi)=(-1)^v$，此处 $v=\sum_i(m_i-1)=n-r$.

(3) 我们注意到 $(12)(23)(12)=(13)$，$(13)(34)(13)=(14)$，等等. 然后参考命题 25.

(4) 考虑 $\gamma^{-r}\tau\gamma^r(r=0,1,\cdots,n-2)$，并利用前面一道题.

(5) 本题第一部分由下面的公式得出：$\prod_{\lambda=1}^{k}(a_1^{(\lambda)}a_2^{(\lambda)}\cdots a_r^{(\lambda)})=(a_1^{(1)}a_1^{(2)}\cdots a_1^{(k)}a_2^{(1)}a_2^{(2)}\cdots a_2^{(k)}a_3^{(1)}\cdots)^k$. 本题第二部分是凯莱定理及 γ^s 是 m/d 阶(见 § 5，命题2)这一事实的推论.

(6) 由命题 22，γ 的共轭类包含 $(n-1)!$ 个元素，因而 $|C(\gamma)|=n$ (见 § 17，命题 7). 但是 $C(\gamma)$ 肯定包含 γ 的 n 个幂，因此它不再包含其他元素.

(7) λ 的共轭类包含 $n!/(n-1)$ 个元素. 因而 $|C(\lambda)|=n-1$；但是 $C(\lambda)$ 包含 λ 的 $n-1$ 个幂.

(8) 假如 Z 是 S_n 的中心，那么 $Z<C(\gamma)\cap C(\lambda)=\{\iota\}$，此处 γ 与 λ 的定义如习题(6)与习题(7).

(9) (i) $a\lambda_u\lambda_v=u^{-1}a\lambda_v=v^{-1}u^{-1}a=(uv)^{-1}a=a\lambda_{uv}$；(ii) $\lambda_u=\iota$，当且

仅当 $u^{-1}a=a$ 对于所有的 $a\in G$,从而 $u=1$; (iii) $a\,\lambda_u\rho_x=u^{-1}ax=a\,\rho_x\lambda_u$ $(a\in G)$;(iv) 设 $a\theta\lambda_u=a\,\lambda_u\theta(a,u\in G)$。令 $a=1$,定义 $x=1\,\theta$,于是 $x\,\lambda_u=1\,\lambda_u\theta$,即 $u^{-1}x=u^{-1}\theta$。因为当 u 遍历 G 时 u^{-1} 也遍历 G,因而 $\theta=\rho_x$,相似地,当 $a\,\eta\rho_x=a\,\rho_x\eta$,$\eta=\lambda_u$,此处 $1\,\eta=u^{-1}$。

(10) 令 $[G:H]=n$.那么存在一个单同态 $\theta:G\to S_n$.因而 $|G\theta|=168\leqslant n!$ 因此 $n\geqslant 6$.

(11) 假如矩形中心在原点,边分别平行 x-轴与 y-轴,那么对称是恒等变换及绕任一坐标轴旋转 π。此群与四群同构。

(12) 在 G 对于 G_1 的陪集展开式中,文字 1 恰好出现在所有不属于 G_1 的置换中,即 1 总共出现 $g-(g/n)$ 次;对于别的文字情况也是相同的。

第 八 章

(1) 群 V(四群)是 A_4 的 4 阶正规子群,因此 V 是 4 阶的唯一西洛群。每一 3-轮换生成一西洛 3-群,例如 1,(123),(132)。共有 4 个这样 3 阶的群,每一个对应于从 A_4 所作用的四个对象中选三个的选择。

(2) 置换 $a=(1234)$ 与 $b=(24)$ 生成一个 8 阶子群,包含下列置换:

(1),(1234),(1432),(24),(13),(12)(34),(13)(24),(14)(23).

这是西洛2-群.因为 $a^4=b^2=(ab)^2=1$,这群与二面体群(§ 14,表 xi)同构。此西洛群显然不是正规的,因而也不是唯一的。共有三个西洛 2-群.

(3) 这样的群必具有八个 7 阶的子群及七个 8 阶的子群,在 56 阶的群中这是不可能的.

(4) 共有 $1+xp$ 个西洛 p-群且 $1+xp\,|\,p^2q$。因而 $1+xp\,|\,q$,这意味 $x=0$。共有 $1+yq$ 个西洛 q-群及 $1+yq\,|\,p^2q$,$1+yq\,|\,p^2$。假如 $y\neq 0$,上式意味 $1+yq$ 等于 p 或 p^2;在两种情况中,都有 $q\,|\,p^2-1$,这是被排除的。因此 $y=0$。因而 $G=P\times Q$,此处 $|P|=p^2$,$|Q|=q$。因为 P 与 Q 是阿贝尔群,所以 G 也是阿贝尔群.

(5) 设 $|G|=p^m g'$,此处 $(g',p)=1$,及 $|K|=p^\mu$。利用 G 对于 K 与任一西洛 p-群 P 的双陪集分解式,即

$$G=Kt_1P\cup Kt_2P\cup\cdots\cup Kt_rP.$$

象在定理29中所证明那样,我们可以证明至少存在一个指标 j,使得 $|t_j^{-1}Pt_j\cap$

$K|=p^{\nu}$，即$K\leqslant t_i^{-1}Pt_i$。

(6) 由习题(5)，$t_iKt_i^{-1}\leqslant P$。因为$K\lhd G$，$t_iKt_i^{-1}=K$，从而$K\leqslant P$。

(7) 设$|G|=p^m s$，此处$(p,s)=1$。于是$|P|=p^m$。而HP是一个群，因为$H\lhd G$，因而$HP=PH$(§ 15，定理 5)。显然$P\leqslant HP$。因而$|HP|=p^m t$，此处$(p,\ t)=1$，而由拉格朗日定理$t\,|\,s$。关系式$HP/H\cong P/H\cap P$(§ 22，定理 10)说明HP/H是p-群，因为右边显然是p-群。(i) 只要证明$|G/H|:|HP/H|$与p互素就足够了。但是这商等于$|G|:|HP|=s:t$，确实与p互素。(ii) 再由定理 10，$|H|:|H\cap P|=|HP|:|P|=t$，象所要求的那样。

参 考 书

Burnside, W., 1911. *Theory of group of finite order*, 2nd edition. (Reprint by Dover Publications, 1955.)

Coxeter, H. S. M., and Moser, W. O., 1965. *Generators and relations for discrete groups*, 2nd edition(Springer).

Hall, Marshall Jr., 1959. *The theory of groups*(Macmillan).(有中译本. 裘光明译,科学出版社,1981.)

Hupert, B., 1967. *Endliche Gruppen* I(Springer).

Kurosh, A. G., *The theory of groups*, 2 vols. (transl. from the Russian by K. A. Hirsch, Chelsea, 1955).

(有中译本. I. 曾肯成、郝钢新译, II. 刘绍学译,高等教育出版社.)

Miller, G. A., Blichfeld, H. F., and Dickson, L. E., 1916. *Theory and application of finite groups* (John Wiley: reprint by Dover Publications, 1961).

Zassenhaus, H., *The theory of groups* (transl. from the German by S. Kraivcty, 2nd edition New York, 1958).

索　引

一　画

二　画

三　画

四　画

五 画

六 画

七 画

八 画

九 画

十 画

十 一 画

十 二 画

十 三 画

十四画以上

［Ｇｅｎｅｒａｌ　Ｉｎｆｏｒｍａｔｉｏｎ］
书名＝群论引论
作者＝（美）Ｗ·莱德曼
页数＝１８５
ＳＳ号＝１００６８９９２
出版日期＝１９８７年１０月第１版